SANbox2-64 Fibre Channel Switch

Installation Guide

Information furnished in this manual is believed to be accurate and reliable. However, QLogic Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic Corporation reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic Corporation makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic Corporation assumes no responsibility for any errors that may appear in this document.

QLogic, SANbox, SANbox2, SANblade, SANsurfer, and Multistage are trademarks or registered trademarks of QLogic Corporation.

Java and Solaris are registered trademarks of Sun Microsystems, Inc.

Pentium III is a registered trademark of Intel Corporation.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows NT, and Windows 2000, and Internet Explorer are trademarks of Microsoft Corporation.

NetScape Navigator is a registered trademark of Netscape Communications Corporation.

Red Hat is a registered trademark of Red Hat Software Inc.

All other brand and product names are trademarks or registered trademarks of their respective owners.

Document Revision History

Revision A, Release, March 2003

© 2000–2003 QLogic Corporation
First Printed: May 2001
All Rights Reserved Worldwide.
Printed in U.S.A.

QLogic Corporation, 6321 Bury Drive, Eden Prairie, MN 55346
(800) 342-7379 or (952) 932-4000

Table of Contents

Section 1 Introduction

1.1 Intended Audience 1-1
1.2 Related Materials 1-2
1.3 Safety Notices 1-3
1.4 Sicherheitshinweise 1-3
1.5 Notes informatives relatives à la sécurité 1-3
1.6 Communications Statements 1-4
1.6.1 Federal Communications Commission (FCC) Class A Statement 1-4
1.6.2 Canadian Department of Communications Class A Compliance Statement 1-4
1.6.3 Avis de conformité aux normes du ministère des Communications du Canada 1-5
1.6.4 CE Statement 1-5
1.6.5 VCCI Class A Statement 1-6
1.6.6 BSMI Class A Statement 1-6
1.7 Laser Safety Information 1-7
1.8 Electrostatic Discharge Sensitivity (ESDS) Precautions 1-7
1.9 Accessible Parts 1-8
1.10 Pièces Accessibles 1-8
1.11 Zugängliche Teile 1-8
1.12 Technical Support 1-9
1.12.1 Availability 1-9
1.12.2 Training 1-9
1.12.3 Contact Information 1-9

Section 2 General Description

2.1 Chassis Hardware 2-2
2.2 Chassis Controls and LEDs 2-4
2.2.1 Maintenance Button 2-5
2.2.1.1 Resetting a Switch 2-5
2.2.1.2 Placing the Switch in Maintenance Mode 2-5
2.2.2 Chassis LEDs 2-6
2.2.2.1 Input Power LED (Green) 2-6
2.2.2.2 Heartbeat LED (Amber) 2-6
2.2.2.3 Fan Fail LED (Amber) 2-7
2.2.2.4 Over Temperature LED (Amber) 2-7

2.3 Fibre Channel Ports 2-7
2.3.1 Small Form-Factor Pluggable (SFP) Transceivers 2-8
2.3.2 Port Status LED 2-8
2.3.3 Port Modes 2-9
2.3.3.1 Fabric Ports 2-9
2.3.3.2 Translated Loop Port 2-10
2.3.3.3 Expansion Port 2-10
2.4 Ethernet Port 2-11
2.5 Serial Port 2-12
2.6 Power Supply Modules 2-13
2.7 Fans 2-14
2.8 Switch Management 2-15

Section 3 Planning

3.1 Devices 3-1
3.1.1 Public and Private 3-1
3.1.2 Redundancy and Latency 3-2
3.2 Multiple Chassis Fabrics 3-4
3.2.1 Domain ID, Principal Priority, and Domain ID Lock 3-4
3.2.2 Common Topologies 3-5
3.3 Performance 3-6
3.3.1 Distance 3-6
3.3.2 Bandwidth 3-7
3.3.3 Latency 3-7
3.4 Device Access 3-8
3.4.1 Soft Zone 3-9
3.4.2 Access Control List Hard Zone 3-9
3.4.3 Virtual Private Fabric Hard Zones 3-10
3.5 Fabric Management 3-10
3.6 Fabric Security 3-11

Section 4 Installation

4.1 Site Requirements 4-1
4.1.1 Fabric Management Workstation 4-1
4.1.2 Switch Power Requirements 4-1
4.1.3 Environmental Conditions 4-2
4.2 Installing a Switch 4-2
4.2.1 Mount the Switch 4-3
4.2.2 Install SFP Transceivers 4-5
4.2.3 Connect the Switch to AC Power 4-5

4.2.4 Connect the Management Workstation to the Switch 4-7
4.2.4.1 Ethernet Connection 4-8
4.2.4.2 Serial Connection 4-8
4.2.5 Installing SANbox Manager 4-9
4.2.6 SANsurfer Management Suite Disk - Windows Installation 4-10
4.2.7 SANsurfer Management Suite Disk - Linux Installation 4-11
4.2.8 SANsurfer Management Suite Disk - Solaris Installation 4-12
4.2.9 SANbox2 Installation Disk - Windows Installation 4-13
4.2.10 SANbox2 Installation Disk - Linux Installation 4-13
4.2.11 SANbox2 Installation Disk - Solaris Installation 4-13
4.2.12 Configure the Switch 4-14
4.2.13 Configure the Ports 4-15
4.2.14 Cable Devices to the Switch 4-15
4.3 Install Firmware 4-16
4.3.1 Using SANbox Manager to Install Firmware 4-16
4.3.2 Using the CLI to Install Firmware 4-17
4.3.3 Using FTP and the CLI to Install Firmware 4-18
4.4 Powering Down a Switch 4-19

Section 5 Diagnostics/Troubleshooting

5.1 POST Diagnostics 5-1
5.1.1 Heartbeat LED Blink Patterns 5-1
5.1.1.1 Normal (all pass) 5-1
5.1.1.2 Maintenance Mode Pattern 5-2
5.1.1.3 Internal Firmware Failure Blink Pattern 5-2
5.1.1.4 Fatal Error Blink Pattern 5-2
5.1.1.5 Configuration File System Error Blink Pattern 5-2
5.1.2 Port Status LED Indications 5-5
5.1.2.1 E_Port Isolation 5-6
5.1.2.2 Excessive Port Errors 5-7
5.2 Chassis Diagnostics 5-9
5.2.1 Over Temperature LED is Illuminated 5-10
5.2.2 Input Power LED Is Extinguished 5-10
5.2.3 Fan Fail LED is Illuminated 5-10
5.2.4 Output Power LED Is Extinguished 5-11
5.2.5 Power Supply Fault LED is Illuminated 5-11
5.3 Recovering a Switch 5-12
5.3.1 Maintenance – Exit 5-13
5.3.2 Maintenance – Image Unpack 5-13
5.3.3 Maintenance – Reset Network Config 5-14

5.3.4 Maintenance – Reset Password File 5-14
5.3.5 Maintenance – Copy Log Files 5-14
5.3.6 Maintenance – Remove Switch Config 5-14
5.3.7 Maintenance – Remake Filesystem 5-14
5.3.8 Maintenance – Reset Switch 5-14

Section 6 Removal/Replacement

6.1 SFP Transceivers 6-1
6.2 CPU Module 6-2
6.2.1 Removing the CPU Module 6-3
6.2.2 Installing the CPU Module 6-5
6.3 I/O Blades 6-7
6.4 Cross-Connect Blades 6-11
6.4.1 Removing a CC Blade 6-12
6.4.2 Installing a CC Blade 6-14
6.5 Power Supply Modules 6-16
6.5.1 Removing a Power Supply Module 6-16
6.5.2 Installing a Power Supply Module 6-17
6.6 Fans 6-18
6.6.1 Removing a Fan 6-18
6.6.2 Installing a Fan 6-19

Appendix A Specifications

A.1 Performance A-1
A.2 Maintainability A-2
A.3 Fabric Management A-3
A.4 Dimensions A-3
A.5 Electrical A-3
A.6 Environmental A-4
A.7 Regulatory Certifications A-4
A.8 Shortwave Laser SFP 1G/2G (multi-mode) A-5
A.9 Longwave Laser SFP 1G/2G (single-mode) A-6

Appendix B Command Line Interface

B.1 Logging On to a Switch B-1
B.2 Command Syntax B-2
B.3 Commands B-3
Admin Command B-4
Alias Command B-5
Config Command B-7

Date Command B-9
Fallback Command B-10
Help Command B-11
History Command B-12
Hotswap Command B-13
Image Command B-15
Lip Command B-16
Passwd Command B-17
Ps Command B-18
Quit Command B-19
Reset Command B-20
Set Command B-25
Set Config Command B-27
Set Log Command B-35
Set Port Command B-38
Set Setup Command B-40
Show Command B-44
Show Config Command B-55
Show Log Command B-58
Show Perf Command B-60
Show Setup Command B-62
Shutdown Command B-65
Test Command B-66
Uptime Command B-69
User Command B-70
Whoami Command B-72
Zone Command B-73
Zoneset Command B-77
Zoning Command B-79

Glossary

Index

Figures

Figure **Page**

2-1 SANbox2-64 64-Port Fibre Channel Switch 2-2
2-2 Slot and Fibre Channel Port Numbering 2-3
2-3 Chassis Controls and LEDS 2-4
2-4 Chassis LEDs 2-6
2-5 Fibre Channel Ports 2-7

2-6 SFP Transceiver 2-8
2-7 Ethernet Port 2-11
2-8 Serial Port 2-12
2-9 Power Supply Components 2-13
2-10 Fans 2-14
3-1 Single Switch Fabric with Initiators and Targets 3-2
3-2 Dual Switch Fabric with Initiators and Targets 3-3
4-1 SANbox2-64 Fibre Channel Switch 4-2
4-2 SANbox2-64 Rail Kit 4-4
4-3 Ethernet and Serial Cable Connections 4-7
5-1 Port Status LED 5-5
5-2 Port Status LED Indications 5-5
5-3 Chassis and Power Supply LEDs 5-9
6-1 Removing the CPU Module 6-4
6-2 Removing an I/O Blade 6-9
6-3 CC Blade Slots 6-11
6-4 Switch Cover Removal 6-13
6-5 CC Blade Removal 6-13
6-6 Installing a CC Blade 6-14
6-7 Removing a Power Supply Module 6-17
6-8 Removing a Fan 6-18

Tables

Table **Page**

2-1 Serial Port Pin Identification 2-12
3-1 Port-to-Port Transmission Combinations 3-7
3-2 Port-to-Port Latency 3-7
4-1 Management Workstation Requirements 4-1
6-1 Marginal Operating Configurations 6-1
B-1 Commands Listed by Authority Level B-3
B-2 Switch Configuration Defaults B-21
B-3 Port Configuration Defaults B-21
B-4 Alarm Threshold Configuration Defaults B-22
B-5 SNMP Configuration Defaults B-23
B-6 System Configuration Defaults B-24
B-7 Set Config Port Parameters B-27
B-8 Set Config Switch Parameters B-29
B-9 Set Config Threshold Parameters B-30
B-10 Set Config Zoning Parameters B-31
B-11 SNMP Configuration Settings B-40
B-12 System Configuration Settings B-41
B-13 Show Port Parameters B-46

Section 1
Introduction

This manual describes the features and installation of the SANbox2-64 Fibre Channel switch, firmware version 1.5. This manual is organized as follows:

- Section 1 describes the intended audience, related materials, safety notices, communications statements, laser safety information, electrostatic discharge sensitivity precautions, accessible parts, and technical support.
- Section 2 is an overview of the switch. It describes indicator LEDs and all user controls and connections.
- Section 3 describes the factors to consider when planning a fabric.
- Section 4 explains how to install and configure the switch.
- Section 5 describes the diagnostic methods and troubleshooting procedures.
- Section 6 describes the removal/replacement procedures for all field replaceable units (FRUs).
- Appendix A lists the switch specifications.
- Appendix B describes the Command Line Interface.

Please read the communications statements and laser safety information later in this section. Use this manual with the *SANbox2-64 Switch Management User's Guide*.

1.1 Intended Audience

This manual introduces users to the switch and explains its installation and service. It is intended for users who are responsible for the installation and servicing of network equipment.

1.2 Related Materials

The following manuals and materials are referenced in the text and/or provide additional information.

- *SANbox2-64 Switch Management User's Guide*, Publication Number 59048-01.
- Fibre Channel-Arbitrated Loop (FC-AL-2) Rev. 6.8.
- Fibre Channel-Private Loop SCSI Direct Attach (FC-PLDA) NCITS TR-19:1998
- Fibre Channel-10-bit Interface Rev. 2.3.
- Definitions of Managed Objects for the Fabric Element in Fibre Channel Standard (draft-ietf-ipfc-fabric-element-mib-04.txt).

The Fibre Channel Standards are available from:

Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112-5776 Phone: (800) 854-7179 or (303) 397-7956
Fax: (303) 397-2740.

1.3
Safety Notices

A **Warning** notice indicates the presence of a hazard that has the potential of causing personal injury.

4-3, 4-5, 6-2, 6-8, 6-12, 6-15, 6-16, 6-18

A **Caution** notice indicates the presence of a hazard that has the potential of causing damage to the equipment.

4-3, 5-14, 6-2, 6-4, 6-8, 6-11, 6-16, 6-18

1.4
Sicherheitshinweise

Ein **Warnhinweis** weist auf das Vorhandensein einer Gefahr hin, die möglicherweise Verletzungen zur Folge hat.

4-3, 4-6, 6-2, 6-8, 6-12, 6-15, 6-16, 6-18

Ein **Vorsichtshinweis** weist auf das Vorhandensein einer Gefahr hin, die möglicherweise Geräteschäden zur Folge hat.

4-3, 5-14, 6-2, 6-4, 6-8, 6-11, 6-16, 6-18

1.5
Notes informatives relatives à la sécurité

Une note informative **Avertissement** indique la présence d’un risque pouvant entraîner des blessures.

4-3, 4-5, 6-2, 6-8, 6-12, 6-15, 6-16, 6-18

Une note informative **Attention** indique la présence d’un risque pouvant entraîner des dégâts matériels.

4-3, 5-14, 6-2, 6-4, 6-8, 6-11, 6-16, 6-18

1.6 Communications Statements

The following statements apply to this product. The statements for other products intended for use with this product appear in their accompanying manuals.

1.6.1 Federal Communications Commission (FCC) Class A Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause unacceptable interference, in which case the user will be required to correct the interference at their own expense.

Neither the provider nor the manufacturer is responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

1.6.2 Canadian Department of Communications Class A Compliance Statement

This equipment does not exceed Class A limits for radio emissions for digital apparatus, set out in Radio Interference Regulation of the Canadian Department of Communications. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps necessary to correct the interference.

1.6.3
Avis de conformité aux normes du ministère des Communications du Canada

Cet équipement ne dépasse pas les limites de Classe A d'émission de bruits radioélectriques por les appareils numériques, telles que prescrites par le Réglement sur le brouillage radioélectrique établi par le ministère des Communications du Canada. L'exploitation faite en milieu résidentiel peut entraîner le brouillage des réceptions radio et télé, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécwssaires pour en éliminer les causes.

1.6.4
CE Statement

The CE symbol on the equipment indicates that this system complies with the EMC (Electromagnetic Compatibility) directive of the European Community (89/336/EEC) and to the Low Voltage (Safety) Directive (73/23/EEC). Such marking indicates that this system meets or exceeds the following technical standards:

- EN60950/A11:1997 – “Safety of Information Technology Equipment, Including Electrical Business Equipment”.
- EN60825-1/A11:1996 – “Safety of Laser Products, Part 1.
- EN55022:1998 – “Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment”.
- EN 55024-1:1998 – “Electromagnetic compatibility - Generic immunity standard Part 1: Residential commercial, and light industry.”
  - IEC1000-4-2:1995 – “Electrostatic Discharge Immunity Test”
  - IEC1000-4-3:1995 – “Radiated, Radio-Frequency, Electromagnetic Field Immunity Test”
  - IEC1000-4-4:1995 – “Electrical Fast Transient/Burst Immunity Test”
  - IEC1000-4-5:1995 – “Surge Immunity Test”
  - IEC1000-4-6:1996 – “Immunity To Conducted Disturbances, Induced By Radio-Frequency Fields”
  - IEC1000-4-8:1993 – Power Frequency Magnetic Field Immunity Test”
  - IEC1000-4-11:1994 – “Voltage Dips, Short Interruptions And Voltage Variations Immunity Tests”
- EN61000-3-2:1995 – “Limits For Harmonic Current Emissions (Equipment Input Current Less Than/Equal To 16 A Per Phase)” Class A
- EN61000-3-3:1995 – “Limitation Of Voltage Fluctuations And Flicker In Low-Voltage Supply Systems For Equipment With Rated Current Less Than Or Equal To 16 A”

1.6.5
VCCI Class A Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council For Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

1.6.6
BSMI Class A Statement

警告使用者:

這是甲類的資訊產品, 在居住的環境中使用時, 可能會造成射頻干擾, 在這種情況下, 使用者會被要求採取某些適當的對策.

Warning:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user will be required to take adequate measures.

1.7

Laser Safety Information

This product may use Class 1 laser optical transceivers to communicate over the fiber optic conductors. The U.S. Department of Health and Human Services (DHHS) does not consider Class 1 lasers to be hazardous. The International Electrotechnical Commission (IEC) 825 Laser Safety Standard requires labeling in English, German, Finnish, and French stating that the product uses Class 1 lasers. Because it is impractical to label the transceivers, the following label is provided in this manual.

1.8

Electrostatic Discharge Sensitivity (ESDS) Precautions

The assemblies used in the switch chassis are ESD sensitive. Observe ESD handling procedures when handling any assembly used in the switch chassis.

1.9 Accessible Parts

The Field Replaceable Units (FRUs) in the SANbox2-64 switch are:

- Small Form-Factor Pluggable (SFP) optical transceivers
- CPU module
- I/O blades
- Power supply modules
- Fans

Refer to Section 6 Removal/Replacement for more information.

1.10 Pièces Accessibles

Les pièces remplaçables, Field Replaceable Units (FRU), du commutateur SANbox2-64 Fibre Channel Switch sont les suivantes:

- Interfaces aux media d'interconnexion appelés SFP transceivers.
- Module d'UC
- Lames d'entrée/sortie
- Modules d'alimentation d'énergie
- Ventilateurs

Se reporter à la Section 6 Removal/Replacement (Procédures de retrait et remplacement) pour plus de renseignements.

1.11 Zugängliche Teile

Nur die folgenden Teile im SANbox2-64 Fibre Channel Switch können kundenseitig ersetzt werden:

- Schnittstellen für die Zwischenverbindungsträger, SFP transceivers genannt.
- Zentraleinheitsmodule
- Blätter Des Einganges/Ausganges
- Netzteilmodule
- Gehäuselüfte

Weitere Informationen finden Sie im Abshcnitt 6 (Ausbauen der ersetzbaren Teile).

1.12 Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic switch products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Visit the QLogic switch support Web site listed in Contact Information for the latest firmware and software updates.

1.12.1 Availability

QLogic Technical Support is available from 7:00 AM to 7:00 PM Central Standard Time, Monday through Friday, excluding QLogic-observed holidays.

1.12.2 Training

QLogic offers the following technical training courses:

- Switch Certification
- HBA Certification

Each course is available at the training facility in Eden Prairie, MN or at your local facility. All courses include a Fibre Channel overview and sections on installation, maintenance, and topology solutions. Each student receives a set of manuals and a CD-ROM containing course training materials. Upon successful completion of the training, Qlogic awards a certificate identifying the student as a Certified SANbox® or SANblade® Professional.

1.12.3 Contact Information

Address:	QLogic Switch Products Inc. 6321 Bury Drive Eden Prairie, Minnesota 55346 USA
Telephone:	+1 952-932-4040
Fax:	+1 952-932-4018
Email: Technical Service Technical Training	 support@qlogic.com tech.training@qlogic.com
Switch Support Web Site:	support.qlogic.com

Notes

Section 2
General Description

This section describes the features and capabilities of the SANbox2-64 Fibre Channel switch. The following topics are described:

- Chassis configuration
- Chassis controls and LEDs
- Fibre channel ports
- Ethernet port
- Serial port
- Fabric management

Fabrics are managed with the SANbox Manager switch management application (version 1.05) and the Command Line Interface (CLI). Refer to Appendix B Command Line Interface for more information. Refer to the*SANbox2-64 Switch Management User's Guide* for information about using the SANbox Manager application.

2.1 Chassis Hardware

The SANbox2-64 switch is set of up to eight 8-port I/O blades. Each I/O blade is interconnected with all other I/O blades through the backplane which is supported by four cross-connect ASICs. A CPU module provides configuration, monitoring, data path management, and control functions.

The base SANbox2-64 switch is configured as a 16-port switch. The 16-port switch is equipped with 2 I/O blades, 2 power supply modules, and a CPU module. To maintain proper air flow and cooling in the 16-port switch, inserts are installed in empty I/O blade slots. You can expand the switch by installing additional I/O blades up to a total of eight. The 64-port switch is equipped with 8 I/O blades, 2 power supply modules, and a CPU module as shown in Figure 2-1. Refer to Section 6 Removal/Replacement for the marginal operating configurations.

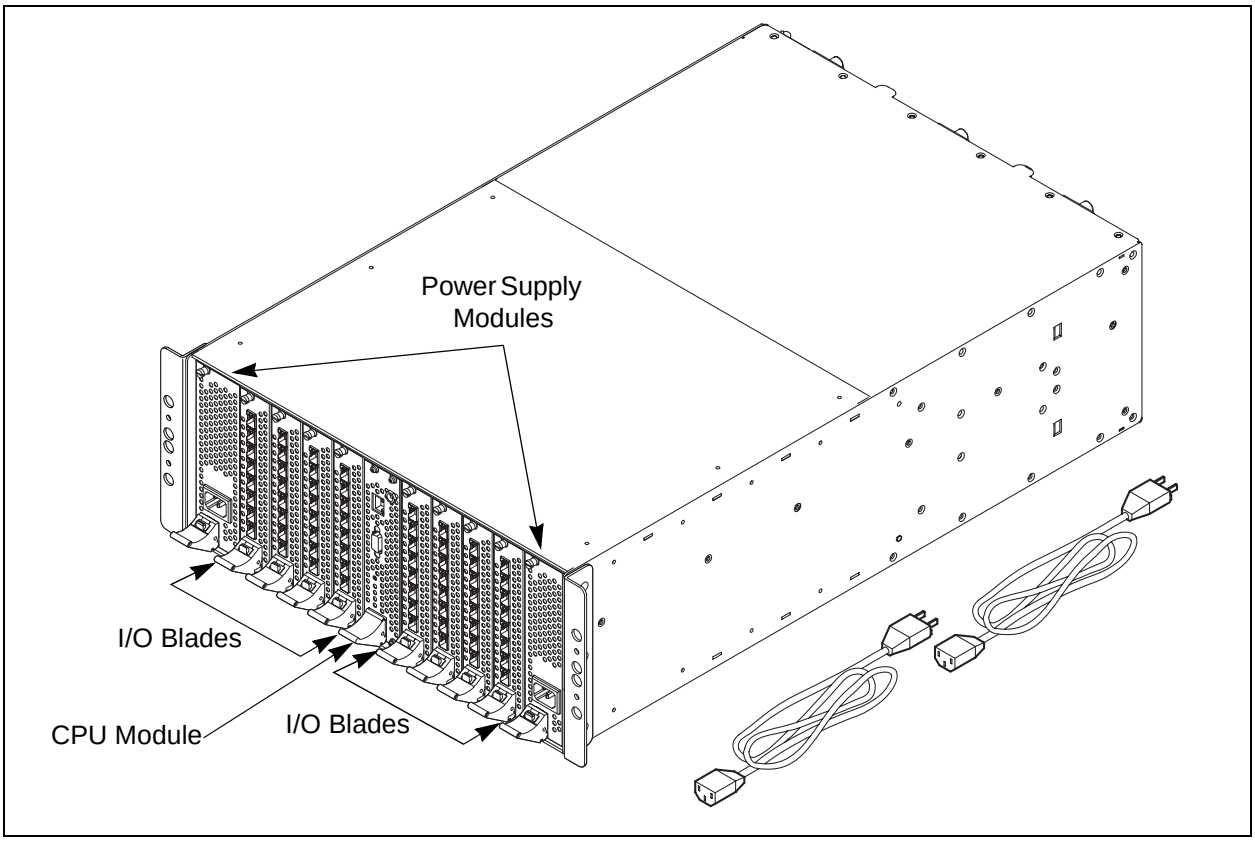


Figure 2-1. SANbox2-64 64-Port Fibre Channel Switch

There are 11 slots numbered #0–#10 as shown in Figure 2-2. Power supply modules occupy slots #0 and #10. The CPU module occupies slot #5. I/O blades occupy slots #1–#4 and #6–#9. The Fibre Channel ports on the I/O blades are numbered 0–63 from top to bottom according to slot number as shown in Figure 2-2. For example, the ports 0–7 are always associated with the I/O blade in slot #1; ports 8–15 are always associated with slot #2, and so on. For example, if there were no I/O blade in slot #1, I/O blade #2 would retain the 8–15 port numbering.

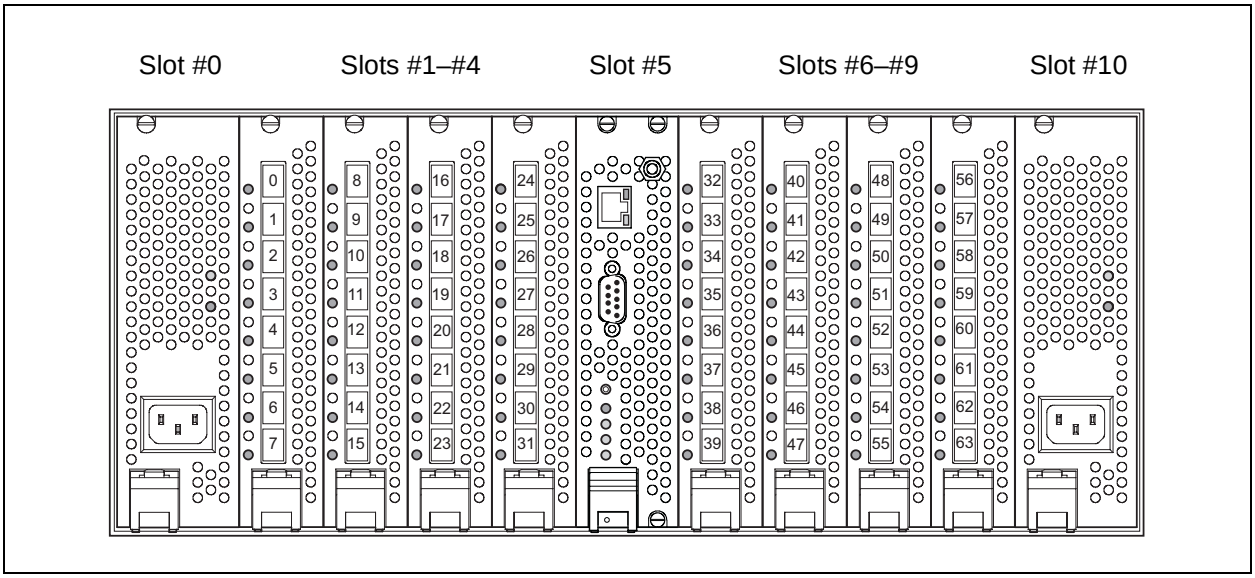


Figure 2-2. Slot and Fibre Channel Port Numbering

The base SANbox2-64 switch comes with I/O blades in slots 1 and 9. You can expand the switch to 24, 32, 40, 48, 56, or 64 ports by installing 1, 2, 3, 4, 5, or 6 additional I/O blades. Install additional I/O blades in open slots in the following order:

- 3rd I/O blade in slot 2
- 4th I/O blade in slot 8
- 5th I/O blade in slot 3
- 6th I/O blade in slot 7
- 7th I/O blade in slot 4
- 8th I/O blade in slot 6

2.2

Chassis Controls and LEDs

The Maintenance button on the CPU module, as shown in Figure 2-3, is the only chassis control. Power is applied to the switch logic circuitry when one or both power supply modules are connected to a 110 or 230 VAC power source. The chassis LEDs are located on the CPU module and provide status information about the condition of the switch. The chassis LEDs include the Input Power LED, Heartbeat LED, Over Temperature LED, and the Fan Fail LED. Refer to "Power Supply Modules" on page 2-13 for information about power supply LEDs and to "Port Status LED" on page 2-8 for information about the Port Status LED.

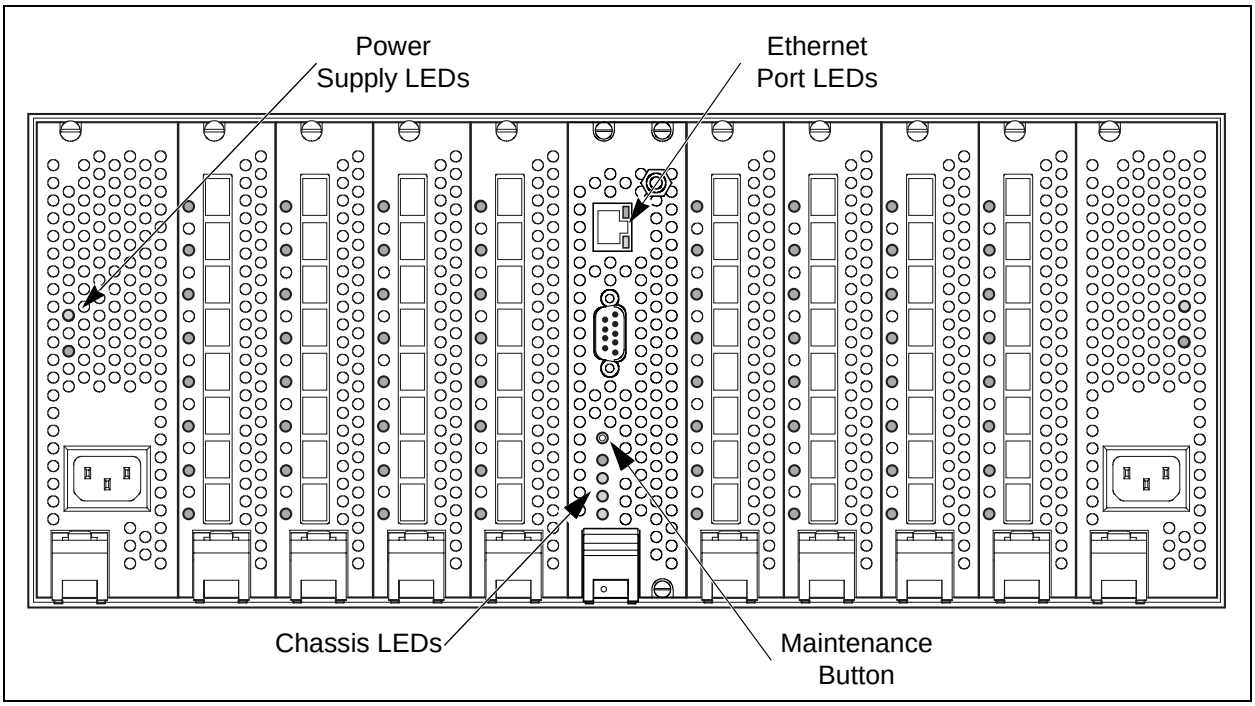


Figure 2-3. Chassis Controls and LEDS

2.2.1
Maintenance Button

The Maintenance button is dual function control on the CPU module that resets the switch or places the switch in maintenance mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes when flash memory or the resident configuration file is corrupted. Refer to ”Recovering a Switch” on page 5-12 for information about maintenance mode.

2.2.1.1
Resetting a Switch

To reset the switch, use a pointed tool to press and release (less than 4 seconds) the Maintenance button. The switch will respond as follows:

1. All of the chassis LEDs will illuminate and then extinguish leaving only the Input Power LED illuminated.
2. After approximately 1 minute, the power-on self test begins illuminating all chassis LEDs.
3. When the POST is complete, the chassis LEDs extinguish leaving the Input Power LED illuminated and the Heartbeat LED flashing once per second.

2.2.1.2
Placing the Switch in Maintenance Mode

To place the switch in maintenance mode, do the following:

1. Isolate the switch from the fabric.
2. Press and hold the Maintenance button with a pointed tool for about 4 seconds. When the Input Power LED alone is illuminated, release the button.
3. After approximately 1 minute, the power-on self test begins illuminating all chassis LEDs.
4. When the POST is complete, the chassis LEDs extinguish leaving the Input Power LED and the Heartbeat LED illuminated. The Heartbeat LED illuminates continuously while the switch is in maintenance mode.

To exit maintenance mode and return to normal operation, press and release the Maintenance button to reset the switch.

2.2.2
Chassis LEDs

The chassis LEDs shown in Figure 2-4 provide status information about switch operation.

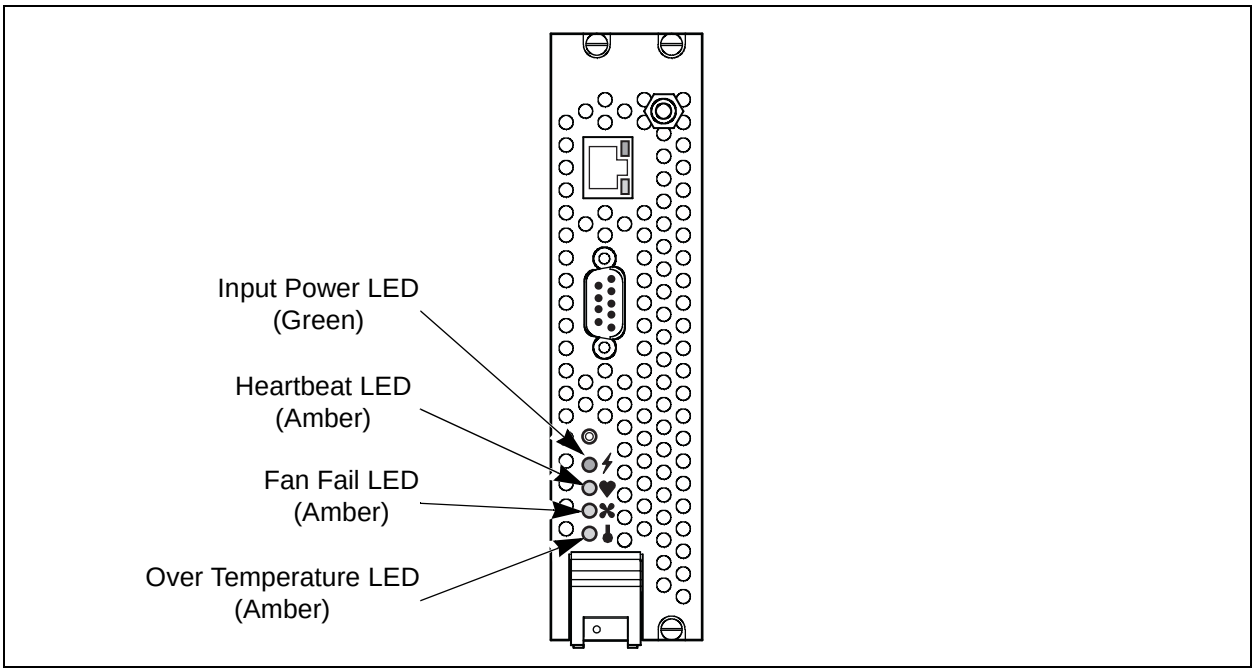


Figure 2-4. Chassis LEDs

2.2.2.1
Input Power LED (Green)

The Input Power LED indicates the voltage status at the switch logic circuitry. This LED illuminates when the switch logic circuitry is receiving the proper DC voltages.

2.2.2.2
Heartbeat LED (Amber)

The Heartbeat LED indicates the status of the internal switch processor and the results of Power On Self Tests (POSTs). Following a normal power-up, the Heartbeat LED blinks about once per second to indicate that the switch passed the POST and that the internal switch processor is running. In maintenance mode, the Heartbeat LED illuminates continuously. Refer to ”Heartbeat LED Blink Patterns” on page 5-1 for more information about Heartbeat LED blink patterns.

2.2.2.3
Fan Fail LED (Amber)

The Fan Fail LED indicates operational status of all fans. This LED illuminates if the speed of any fan falls below the normal range. Removing a fan will not illuminate the Fan Fail LED. Refer to Section 5 Diagnostics/Troubleshooting for information about troubleshooting fan failure conditions.

2.2.2.4
Over Temperature LED (Amber)

The Over Temperature LED provides status information about the air temperature inside the switch. This LED illuminates to indicate that the switch logic circuitry is overheating. Refer to Section 5 Diagnostics/Troubleshooting for information about troubleshooting over temperature conditions.

2.3
Fibre Channel Ports

Each I/O blade has eight Fibre Channel ports that are interconnected with all other I/O blades through the backplane. Fibre Channel ports are numbered according to the slot in which the I/O blade resides. Each port is served by a Small Form-Factor Pluggable (SFP) transceiver. A Port Status LED, located to the left of each port as shown in Figure 2-5, provides port login and activity status information. Port modes configure the ports to communicate with public devices, private devices, and other switches.

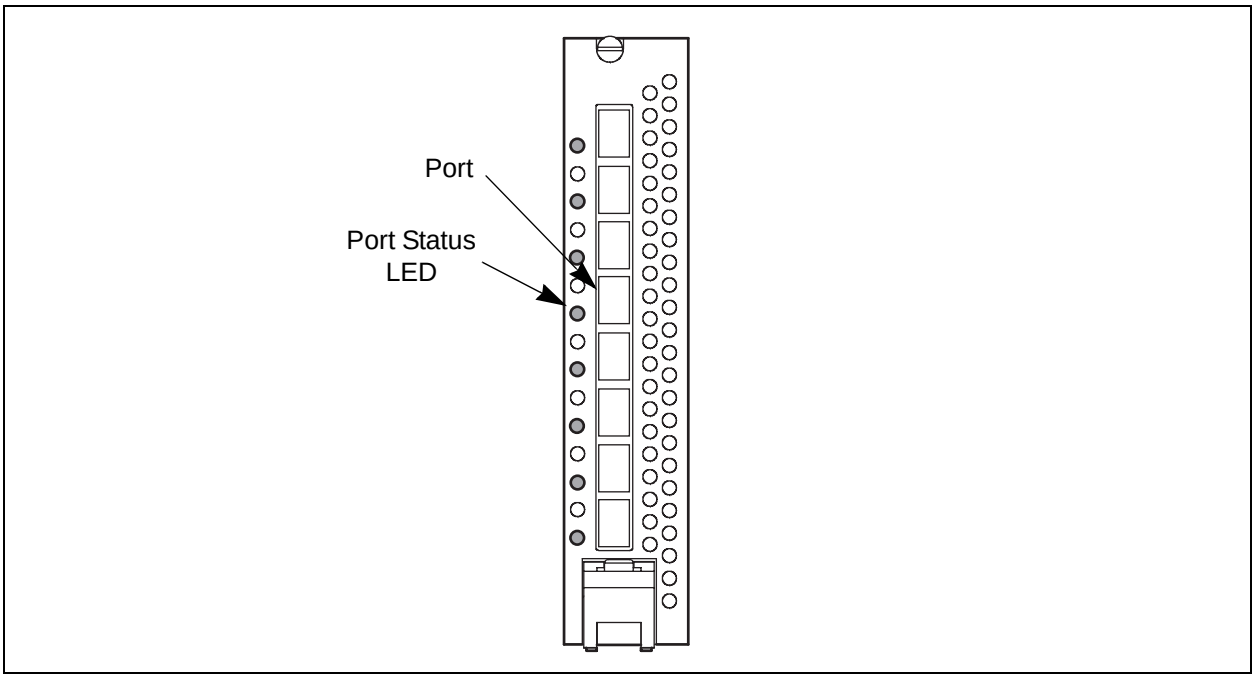


Figure 2-5. Fibre Channel Ports

2.3.1
Small Form-Factor Pluggable (SFP) Transceivers

An SFP transceiver, like the one shown in Figure 2-6, converts electrical signals to and from optical laser signals to transmit and receive data. SFP transceivers plug into the ports; duplex fiber optic cables plug into the transceivers which then connect to the devices. A port is capable of transmitting at 1 Gbps or 2 Gbps; however, the transceiver must be capable of 2 Gbps for the port to deliver at that rate.

The SFP transceivers are hot swappable. This means that you can remove or install an SFP transceiver while the switch is operating without harming the switch or the transceiver. However, communication with the connected device will be interrupted. Refer to Section 6 Removal/Replacement for information about installing and removing SFP optical transceivers.

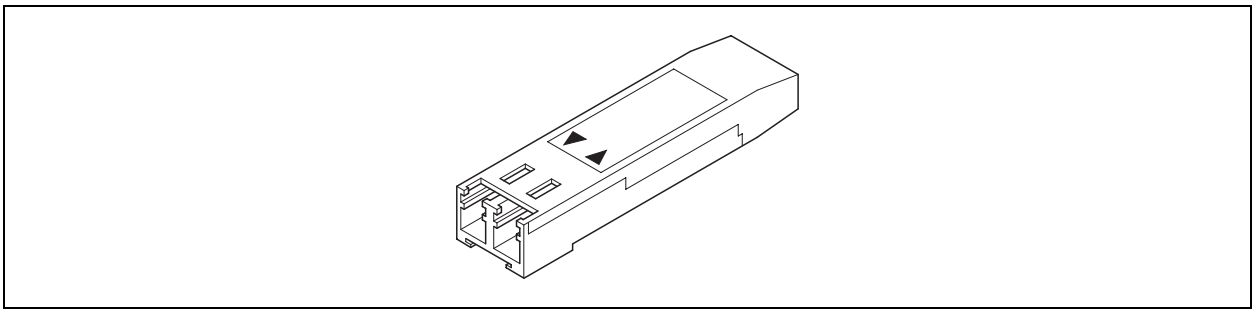


Figure 2-6. SFP Transceiver

2.3.2
Port Status LED

The Port Status LED is a two-color LED that indicates both logged-in (or loop initialization) status and when the port is transmitting or receiving frames. Following a successful port login or loop initialization, the Port Status LED illuminates green. When the port begins transmitting or receiving frames, the Port Status LED illuminates amber for 50 milliseconds as each frame passes. This makes it possible to observe the transmission of a single frame. The Port Status LED remains illuminated as long as the port is initialized or logged in. If the port connection is broken or an error occurs that disables the port, the Port Status LED will flash green. Refer to ”Port Status LED Indications” on page 5-5 for more information about the Port Status LED.

2.3.3
Port Modes

SANbox2-64 switches support the following port modes:

- Generic ports (GL_Port and G_Port)
- Fabric ports (FL_Port and F_Port)
- Translated loop ports (TL_Port)
- Expansion ports (E_Port)

Switches come from the factory with all ports configured as GL_Ports. GL_Ports self-configure in the following ways:

- FL_Port when connected to a loop of public devices
- F_Port when connected to a single public device. If the device is a single device on a loop, the GL_Port will attempt to configure first as an F_Port, then if that fails, as an FL_Port.
- E_Port when connected to another FC-SW-2 compliant switch

G_Ports self-configure in the following ways:

- F_Port when connected to a public device
- E_Port when connected to another FC-SW-2 compliant switch

A TL_Port supports private loop devices and must be configured explicitly. Refer to the *SANbox2-64 Switch Management User's Guide* for more information about defining port modes.

2.3.3.1
Fabric Ports

An FL_Port can support a loop of up to 126 public devices. An FL_Port can also configure itself during the fabric login process as an F_Port when connected to a single public device (N_Port).

2.3.3.2
Translated Loop Port

A TL_Port supports a loop of up to 125 private initiator devices or up to 124 private target devices with the ability to communicate with “off-loop” devices. This includes public fabric devices and private devices on other TL_Ports. TL_Ports connect to devices that conform to the Fibre Channel-Private Loop SCSI Direct Attach (FC-PLDA) standard. Devices connected to TL_Ports are registered with the Name Server.

A TL_Port acts as a proxy for the off-loop device translating private frames into and from public frames. Each TL_Port can proxy up to 63 off-loop initiator devices or up to 64 off-loop target and initiator devices. The set of off-loop devices are maintained in the TL_Port’s translation entries list.

- For a TL_Port connected to private target devices, the switch firmware automatically creates an entry in the translation entries list for each off-loop initiator device that attempts to establish communication. Soft or VPF zoning can be used to limit the number of potential initiators to 63. Zone membership must be done by worldwide name, or domain ID and port ID.
- For a TL_Port connected to private initiator devices, the switch firmware automatically creates an entry in the translation entries list for up to 64 target and initiator devices that are members of the same soft or VPF zone. Zone membership must be done by worldwide name, or domain ID and port ID.

2.3.3.3
Expansion Port

E_Ports enable you to expand the fabric by connecting SANbox2-64 switches with other FC-SW-2 compliant switches. SANbox2-64 switches self-discover all inter-switch connections. Refer to ”Multiple Chassis Fabrics” on page 3-4 for more information about multiple chassis fabrics.

2.4 Ethernet Port

The Ethernet port is a RJ-45 connector located on the CPU module as shown in Figure 2-7. This port requires a 10/100BASE-T cable and provides a connection for a management workstation, such as a PC, a Solaris™ workstation, or a Linux® workstation, through which to manage the switch. You can manage the switch over an Ethernet connection using SANbox Manager, the Command Line Interface (CLI), or SNMP. The switch through which a fabric is managed is called the fabric management switch.

The Ethernet port has two LEDs: a Link Status LED and an Activity LED. The Link Status LED illuminates green to indicate that an Ethernet connection has been established with a management workstation. The Activity LED illuminates amber to indicate that data is being transmitted or received over the Ethernet connection.

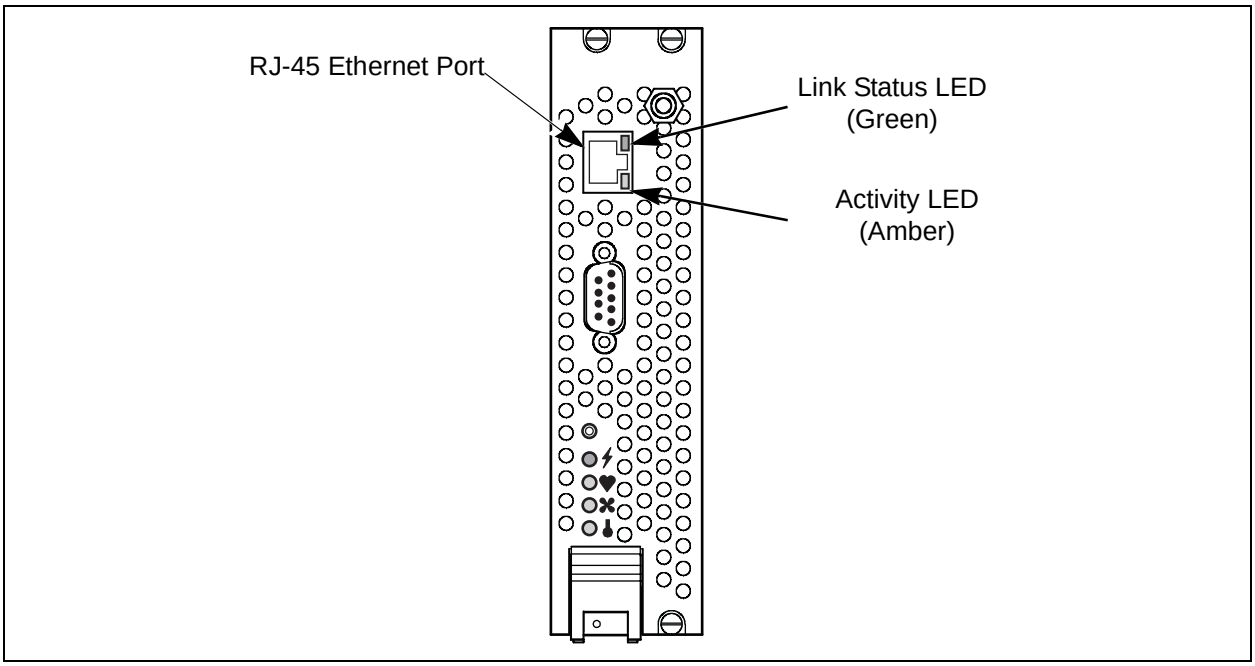


Figure 2-7. Ethernet Port

2.5 Serial Port

The SANbox2-64 switch is equipped with an RS-232 serial port for maintenance purposes. The serial port is located on the CPU module as shown in Figure 2-8.

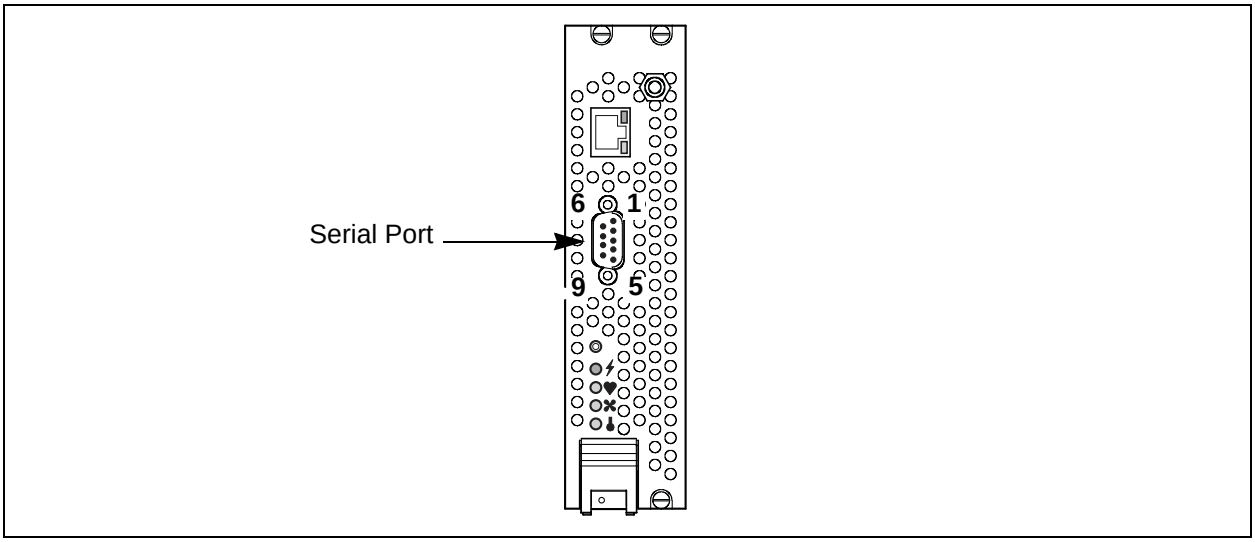


Figure 2-8. Serial Port

The serial port connector requires a null-modem F/F DB9 cable. The pins on the switch RS-232 connector, shown in Figure 2-8, are identified in Table 2-1. Refer to "Connect the Management Workstation to the Switch" on page 4-7 for information about connecting the management workstation through the serial port.

Table 2-1. Serial Port Pin Identification

Pin Number	Description
1	Carrier Detect (DCD)
2	Receive Data (RxD)
3	Transmit Data (TxD)
4	Data Terminal Ready (DTR)
5	Signal Ground (GND)
6	Data Set Ready (DSR)
7	Request to Send (RTS)
8	Clear to Send (CTS)
9	Ring Indicator (RI)

2.6

Power Supply Modules

The power supply modules convert standard 110 or 230 VAC to DC voltages for the various switch circuits. Each power supply module has an AC power receptacle and two status LEDs as shown in Figure 2-9. Each power supply module is capable of providing all of the switch's power needs. During normal operation, each power supply provides half of the demand. If one power supply goes offline, the second power supply steps up and provides the difference. After connecting a power supply to an AC voltage source, the power supply is energized and the DC voltages are delivered to the switch logic circuitry.

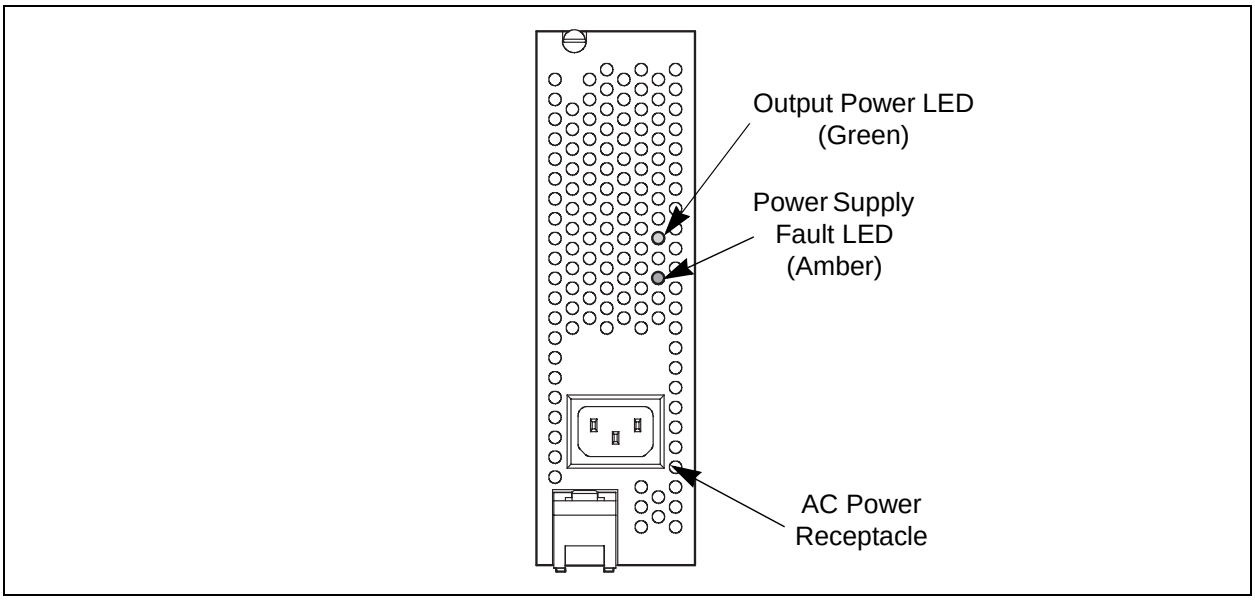


Figure 2-9. Power Supply Components

The power supplies are hot pluggable and interchangeable. Hot pluggable means that you can remove and replace one of the two operating power supplies while the switch is in operation without disrupting service. Refer to Section 6 Removal/ Replacement for information about replacing a power supply.

Each power supply has two status LEDs: a Power Supply Fault LED (amber) and an Output Power LED (green). The Power Supply Fault LED illuminates to indicate a power supply fault. Possible power supply faults include high temperature, high or low input voltage, high or low output voltage, and high current. Refer to Section 5 Diagnostics/Troubleshooting for information about troubleshooting power supply fault conditions.

The Output Power LED illuminates to indicate that the power supply is producing DC voltage at the proper levels.

2.7 Fans

The switch is equipped with three fans as shown in Figure 2-10. If one of the fans should fail, the other two fans are capable of providing the necessary cooling until the failed fan can be replaced. The fans are hot pluggable and interchangeable. Refer to ”Fans” on page 6-18 for information about removing and replacing the fans. Air flow can be back-to-front or front-to-back depending on the model.

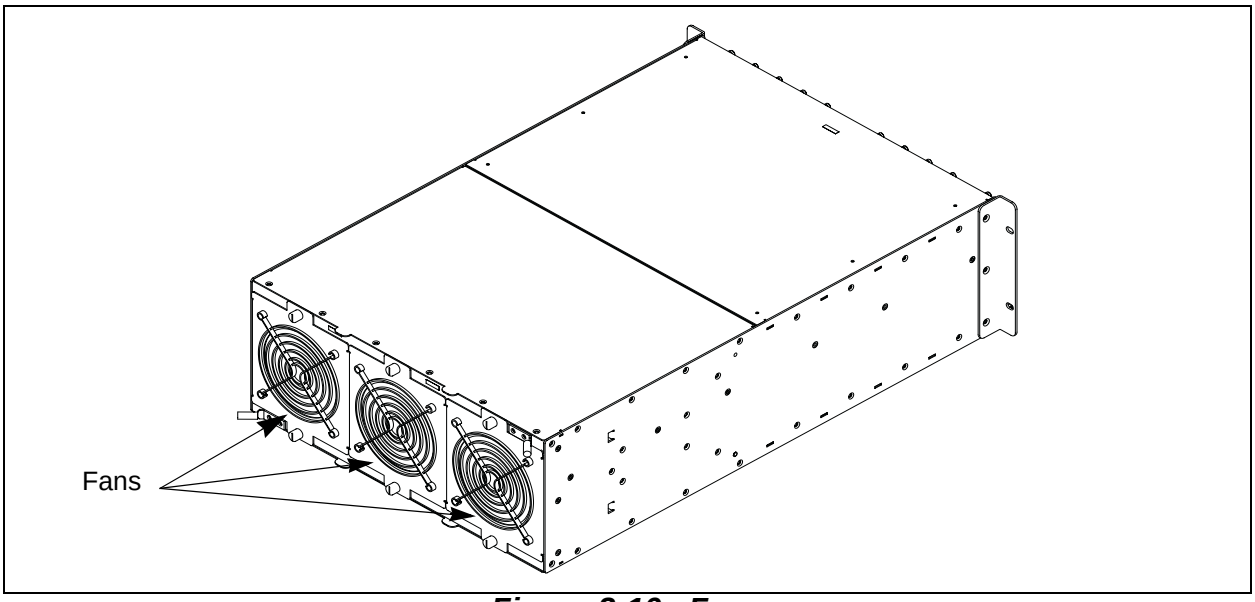


Figure 2-10. Fans

2.8 Switch Management

SANbox Manager is a workstation-based Java® application that provides a graphical user interface for fabric management. This application runs on a Windows®, Solaris, or Linux workstation. The management workstation connects to the switch through the switch's Ethernet port. Refer to the *SANbox2-64 Switch Management User's Guide* for information about the SANbox Manager application and its use.

In addition to SANbox Manager, the switch supports the following management tools:

- Command Line Interface (CLI)
- File Transfer Protocol (FTP)
- Simple Network Management Protocol (SNMP)

The CLI provides monitoring and configuration functions by which the administrator can manage the fabric and its switches. The CLI is available over an Ethernet connection or a serial connection. Refer to Appendix B Command Line Interface for more information.

FTP provides the command line interface for exchanging files between the switch and the management workstation. These files include firmware image files, configuration files, and log files.

SNMP provides monitoring and trap functions for the fabric. SANbox2-64 firmware supports SNMP Versions 1 and 2, the Fibre Alliance Management Information Base (FA-MIB) version 4.0, and the Fabric Element Management Information Base (FE-MIB) RFC 2837. Traps are formatted using SNMP version 2.

Notes

Section 3
Planning

Consider the following when planning a fabric:

- Devices
- Multiple chassis fabrics
- Performance
- Device access
- Fabric management
- Fabric security

3.1 Devices

When planning a fabric, consider the number of devices, the types of device (public or private), and the anticipated demand. This will determine the number of ports that are needed and in turn the number of switches. Consider how many switches are needed and how to connect the devices.

The SANbox2-64 Fibre Channel switch uses SFP optical transceivers, but the device host bus adapters you are using may not. Consider whether the device adapters use SFP transceivers or Gigabit Interface Converters (GBIC), and choose fiber optic cable accordingly. Use LC-type cable connectors for SFP transceivers and SC-type cable connectors for GBIC transceivers.

3.1.1 Public and Private

Consider the distribution of public and private devices as well as targets and initiators. Public devices have full Fibre Channel addressing capability, and therefore can communicate with any other public device on the fabric. An F_Port supports a single public device. An FL_Port can support up to 126 public devices.

Private devices do not have full Fibre Channel addressing capability, only the Arbitrated Loop Physical Address (ALPA) portion. A TL_Port provides a proxy for a loop of private initiator or target devices allowing communication with off-loop public and private devices. Consider the number of private devices in the fabric and the number of off-loop devices with which the private devices must communicate:

- A TL_Port can support up to 125 private initiator devices and maintain communications with up to 64 off-loop target devices.
- A TL_Port can support up to 124 private target devices and maintain communications with up to 63 off-loop initiator devices.

3.1.2
Redundancy and Latency

When planning a fabric, consider how to create redundant paths and minimize latency. Initiators and targets experience the least amount of latency when connected to the same I/O blade. For example, connecting initiator and target “A” ports together on one I/O blade and initiator and target “B” ports on another I/O blade, as shown in Figure 3-1, creates redundant paths and minimizes latency.

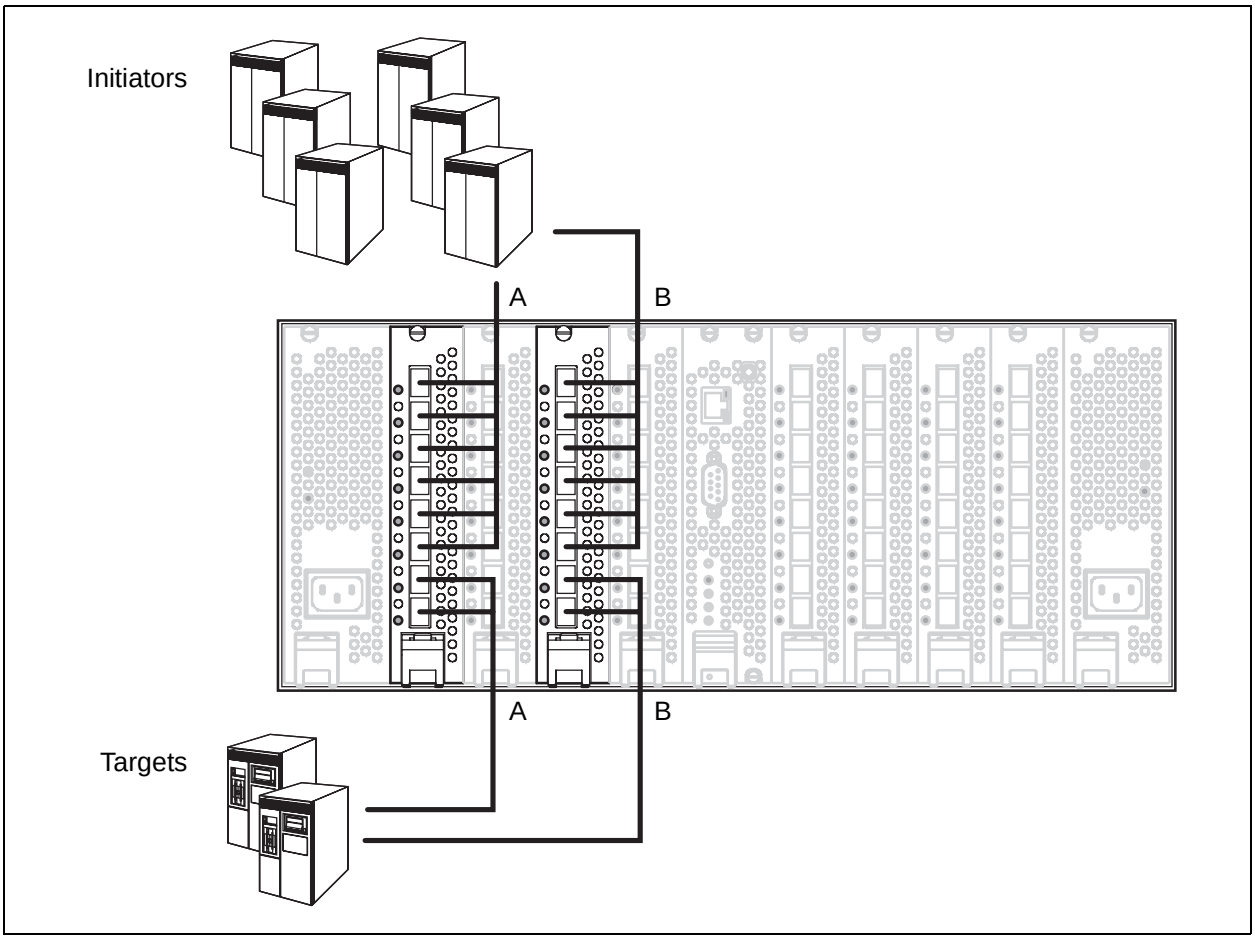


Figure 3-1. Single Switch Fabric with Initiators and Targets

For a multiple switch fabrics in which initiators on one switch communicate with targets on another, the same principles apply as shown in Figure 3-2. The “A” port initiators and E_Ports are grouped together on one I/O blade with connections to the corresponding “A” port targets and E_Ports on the same I/O blade on the second switch. “B” port initiators, targets, and links are connected in a similar way.

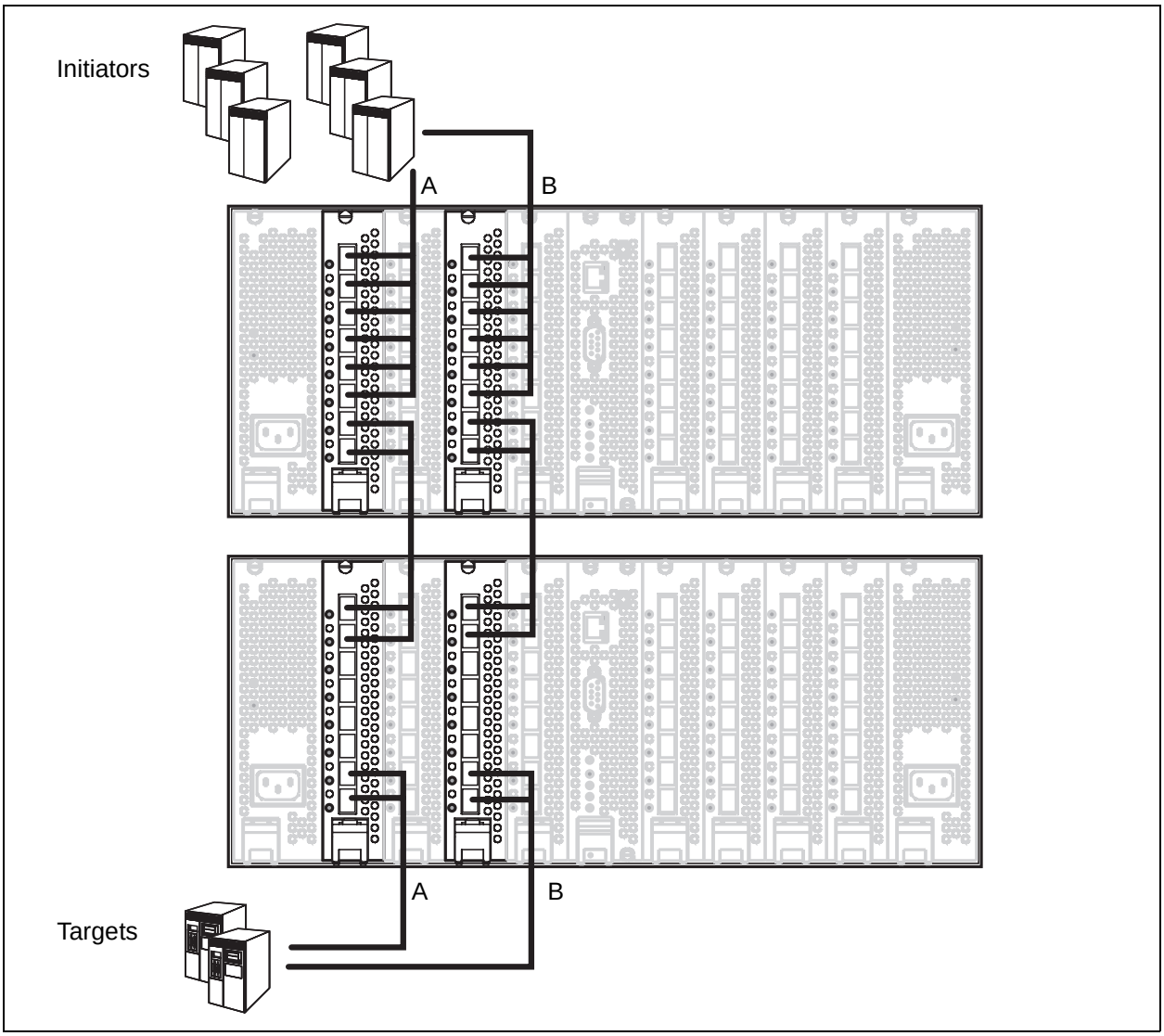


Figure 3-2. Dual Switch Fabric with Initiators and Targets

3.2 Multiple Chassis Fabrics

By connecting switches together you can expand the number of available ports for devices. Each switch in the fabric is identified by a unique domain ID, and the fabric will automatically resolve domain ID conflicts. Because the ports are self-configuring, you can connect SANbox2-64 and other FC-SW-2 compliant switches together in a wide variety of topologies.

3.2.1 Domain ID, Principal Priority, and Domain ID Lock

The following switch configuration settings affect multiple chassis fabrics:

- Domain ID
- Principal priority
- Domain ID lock

The domain ID is a unique number from 1– 239 that identifies each switch in a fabric. The principal priority is a number (1 – 255) that determines the principal switch which manages domain ID assignments for the fabric. The switch with the highest principal priority (1 is high, 255 is low) becomes the principal switch. If the principal priority is the same for all switches in a fabric, the switch with the lowest WWN becomes the principal switch.

The domain ID lock allows (FALSE) or prevents (TRUE) the reassignment of the domain ID on that switch. Switches come from the factory with the domain ID set to 1, the domain ID lock set to FALSE, and the principal priority set to 254. Refer to the *SANbox2-64 Switch Management User's Guide* for information about changing the domain ID using SANbox Manager. Refer to "Set Config Command" on page B-27 (Switch keyword) for information about changing the default domain ID, domain ID lock, and principal priority parameters.

An unresolved domain ID conflict means that the switch with the higher WWN will isolate as a separate fabric, and the Port Status LED status on both switches will flash green to show the affected ports. If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain ID conflict occurs, the new switch will isolate as a separate fabric. However, you can remedy this by resetting the new switch or taking it offline then back online. The principal switch will reassign the domain ID and the switch will join the fabric.

Note: Domain ID reassignment is not reflected in zoning that is defined by domain ID/port number pair or Fibre Channel address. You must reconfigure zones that are affected by domain ID reassignment. To prevent zoning definitions from becoming invalid, use the Set Config Switch command to lock domain IDs. Refer to "Set Config Command" on page B-27.

3.2.2
Common Topologies

The SANbox2-64 switch supports describes three commonly used fabric topologies:

- Cascade
- Mesh
- Multistage®

A cascade topology describes a fabric in which the switches are connected in a linear fashion. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology. The loop reduces latency because any switch can route traffic in the shortest direction to any switch in the loop. The loop also provides failover should a switch fail.

A mesh topology describes a fabric in which each chassis has at least one port directly connected to every chassis in the fabric.

A Multistage topology describes a fabric in which two or more edge switches connect to one or more core switches. Each additional core switch increases the bandwidth to each edge switch by 200 MB/s.

3.3 Performance

The SANbox2-64 switch supports class 2 and class 3 Fibre Channel service at transmission rates of 1 Gbps or 2 Gbps with a maximum frame size of 2148 bytes. A port can transmit or receive at 1 Gbps or 2 Gbps depending on the device to which it is connected. The port discovers the transmission speed prior to login when the connected device powers up. Related performance characteristics include the following:

- Distance
- Bandwidth
- Latency

3.3.1 Distance

Consider the physical distribution of devices and switches in the fabric. Choose SFP transceivers that are compatible with the cable type, distance, Fibre Channel revision level, and the device host bus adapter. Refer to Appendix A Specifications for more information about cable types and SFP transceivers.

Each port is supported by a data buffer with a 12 credit capacity; that is, 12 maximum sized frames. For fibre optic cables, this enables full bandwidth over a distance of 20 kilometers at 1 Gbps (0.6 credits/Km), or 10 kilometers at 2 Gbps (1.2 credits/Km). Beyond this distance, however, there is some loss of efficiency because the transmitting port must wait for an acknowledgement before sending the next frame.

Longer distances can be spanned at full bandwidth by extending credits on G_Ports and F_Ports. Each port can donate up to 11 credits to a pool from which a recipient port on the same I/O blade can borrow. For example, you can configure a recipient port to borrow up to 66 credits from 6 ports for a total of 78 credits. This will support communication over approximately 130 Km at 1 Gbps (78÷0.6) or 65 Km at 2 Gbps (78÷1.2).

You can configure recipient and donor ports using SANbox Manager or the Set Config command. Refer to the ”Set Config Command” on page B-27 for more information.

3.3.2 Bandwidth

Bandwidth is a measure of the volume of data that can be transmitted at a given transmission rate. A port can transmit or receive at 1 Gbps or 2 Gbps depending on the device to which it is connected. The switch supports all transmission rate combinations as shown in Table 3-1.

Table 3-1. Port-to-Port Transmission Combinations

Source Port Rate	Destination Port Rate	Maximum Bandwdith
1 Gbps	1 Gbps	100 MB
1 Gbps	2 Gbps	100 MB
1 Gbps x 2 ports	2 Gbps	200 MB
2 Gbps	1 Gbps x 2 ports	100 MB each port[1]
2 Gbps	2 Gbps	200 MB

[1]Bandwidth will be less for larger sequence sizes.

In multiple chassis fabrics, each link between chassis contributes 100 or 200 megabytes of bandwidth between those chassis. When additional bandwidth is needed between devices, increase the number of links between the connecting switches. The switch guarantees in-order-delivery with any number of links between chassis.

3.3.3 Latency

Latency is a measure of how fast a frame travels from one port to another. The factors that affect latency include transmission rate and the source/destination port relationship as shown in Table 3-2.

Table 3-2. Port-to-Port Latency

Source/Destination Rates	Same I/O Blade
1 Gbps - 1 Gbps	<1 µsec
2 Gbps - 2 Gbps	<0.5 µsec

3.4 Device Access

Consider device access needs within the fabric. Access is controlled by the use of zones and zone sets. Some zoning strategies include the following:

- Separate devices that use different operating systems.
- Separate devices that have no need to communicate with other devices in the fabric or have classified data.
- Separate devices into department, administrative, or other functional group.
- Group TL_Port devices with targets and initiators to allow automatic discovery.
- Reserve a path and its bandwidth from one port to another.

A zone is a named group of devices that can communicate with each other. Membership in a zone can be defined by switch port number, port Fibre Channel address, or by device worldwide name (WWN). Devices can communicate only with devices that are members of the same zone. A zone can be a member of more than one zone set. Several zone sets can be defined for a fabric, but only one zone set can be active at one time. The active zone set determines the current fabric zoning.

A zoning database is maintained on each switch consisting of all inactive zone sets, the active zone set, all zones, aliases, and their membership. The SANbox2-64 switch supports the following maximum limits:

- 256 zone sets
- 256 zones per zone set
- 1000 total zones
- 2000 members per zone
- 256 aliases
- 2000 members per alias
- 2000 total number of alias and zone members

The following types of zones are supported:

- Soft zone
- Access Control List (ACL) - hard zone
- Virtual Private Fabric (VPF) - hard zone

3.4.1
Soft Zone

Soft zoning divides the fabric for purposes of controlling discovery. Members of the same soft zone automatically discover and communicate freely with all other members of the same zone. The soft zone boundary is not secure; traffic across soft zones can occur if addressed correctly. The following rules apply to soft zones:

- Soft zones that include members from multiple switches need not include the ports of the inter-switch links.
- Soft zone boundaries yield to ACL and VPF zone boundaries.
- Soft zones can overlap; that is, a port can be a member of more than one soft zone.
- Membership can be defined by Fibre Channel address, port ID and domain ID, or worldwide name.
- Soft zoning supports all port modes.

3.4.2
Access Control List Hard Zone

Access Control List (ACL) zoning divides the fabric for purposes of controlling discovery and inbound traffic. ACL zoning is a type of hard zoning that is hardware enforced. This type of zoning is useful for controlling access to certain devices without totally isolating them from the fabric. Members can communicate with each other and transmit outside the ACL zone, but cannot receive inbound traffic from outside the zone. The following rules apply to ACL zones:

- The ACL zone boundary is secure against inbound traffic.
- ACL zones can overlap; that is, a port can be a member of more than one ACL zone.
- ACL zones that include members from multiple switches need not include the ports of the inter-switch links.
- ACL zone boundaries supersede soft zone boundaries, but yield to VPF zone boundaries.
- Membership can be defined only by domain ID and port ID.
- ACL zoning supports all port modes except TL_Port.

3.4.3
Virtual Private Fabric Hard Zones

Virtual Private Fabric (VPF) zoning divides the fabric for purposes of controlling discovery and both inbound and outbound traffic. This type of zoning is useful for providing security and reserving paths between devices to guarantee bandwidth. VPF zoning is a type of hard zoning that is hardware enforced. Members can only transmit to and receive from members of the same VPF zone. The VPF zone boundary is secure against both inbound and outbound traffic. The following rules apply to VPF zones:

- VPF zones that include members from multiple switches must include the ports of the inter-switch links.
- VPF zones cannot cross I/O blades.
- VPF zones cannot overlap; that is, a port can be a member of only one VPF zone.
- VPF zone boundaries supersede both soft and ACL zone boundaries.
- Membership can be defined only by domain ID and port ID.
- VPF zoning supports all port modes.

3.5
Fabric Management

The SANbox Manager application and CLI execute on a management workstation that provides for the configuration, control, maintenance of the fabric. Supported platforms include Windows, Windows NT, Solaris, and Linux. The SANbox Manager application can manage multiple fabrics. Consider how many fabrics will be managed, how many management workstations are needed, and whether the fabrics will be managed with the CLI or SANbox Manager.

The switch supports a combined maximum of 15 logins. This includes SANbox Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins and Telnet logins. Of this 15, there can be a combined maximum of 10 SANbox Manager and API logins. Additional logins will be refused.

3.6

Fabric Security

You manage fabric security on a switch basis through the creation of user accounts. Each account consists of an account name, a password, and an authority level. There are two authority levels: User and Admin. These authority levels apply to SANbox Manager and to the CLI. User authority permits only monitoring and display tasks. Admin authority permits all management tasks including user administration. Consider your fabric security needs, who the system administrators will be, and authority levels they should have.

- Refer to ”Commands” on page B-3 for more information about authority levels.
- Refer to the ”User Command” on page B-70 for information about creating user accounts.
- Refer to the ”Set Setup Command” on page B-40 and the System keyword for information about fabric security and the enforcement of user accounts.

Notes

Section 4

Installation

This section describes how to install and configure the SANbox2-64 switch. It also describes how to load new firmware and how to recover a disabled switch.

4.1

Site Requirements

The following items are required for the installation of a SANbox2-64 switch:

- Fabric management workstation
- Power requirements
- Environmental conditions

4.1.1

Fabric Management Workstation

The requirements for fabric management workstations running SANbox Manager are described in Table 4-1:

Table 4-1. Management Workstation Requirements

Operating System	■ Windows® NT, 2000, 95/98 ■ Linux® 6.2 Red Hat® ■ Solaris
Memory	128 MB or more
Disk Space	150 MB per installation
Processor	300 MHz or faster
Hardware	CD-ROM drive, RS-232 serial port, RJ-45 Ethernet port
Internet Browser	Microsoft® Internet Explorer® or Netscape Navigator®

Telnet workstations require an RJ-45 Ethernet port or an RS-232 serial port and an operating system with a Telnet client.

4.1.2

Switch Power Requirements

Operating voltage requirements are as follows:

90 to 264 Vac; 47 to 63 Hz

4.1.3
Environmental Conditions

Consider the factors that affect the climate in your facility such as equipment heat dissipation and ventilation. The switch requires the following operating conditions:

- Operating temperature range: 5° to 40° C (41°- 104°F)
- Relative humidity: 15% - 80%, non-condensing

4.2
Installing a Switch

Unpack the switch and accessories. The SANbox2-64 product is shipped with the components shown in Figure 4-1:

- SANbox2-64 Fibre Channel Switch with firmware installed
- Power cords (2)
- Rack mount brackets (2)
- Rail kit (1)
- CD containing the SANbox Manager switch management application, release notes, and documentation

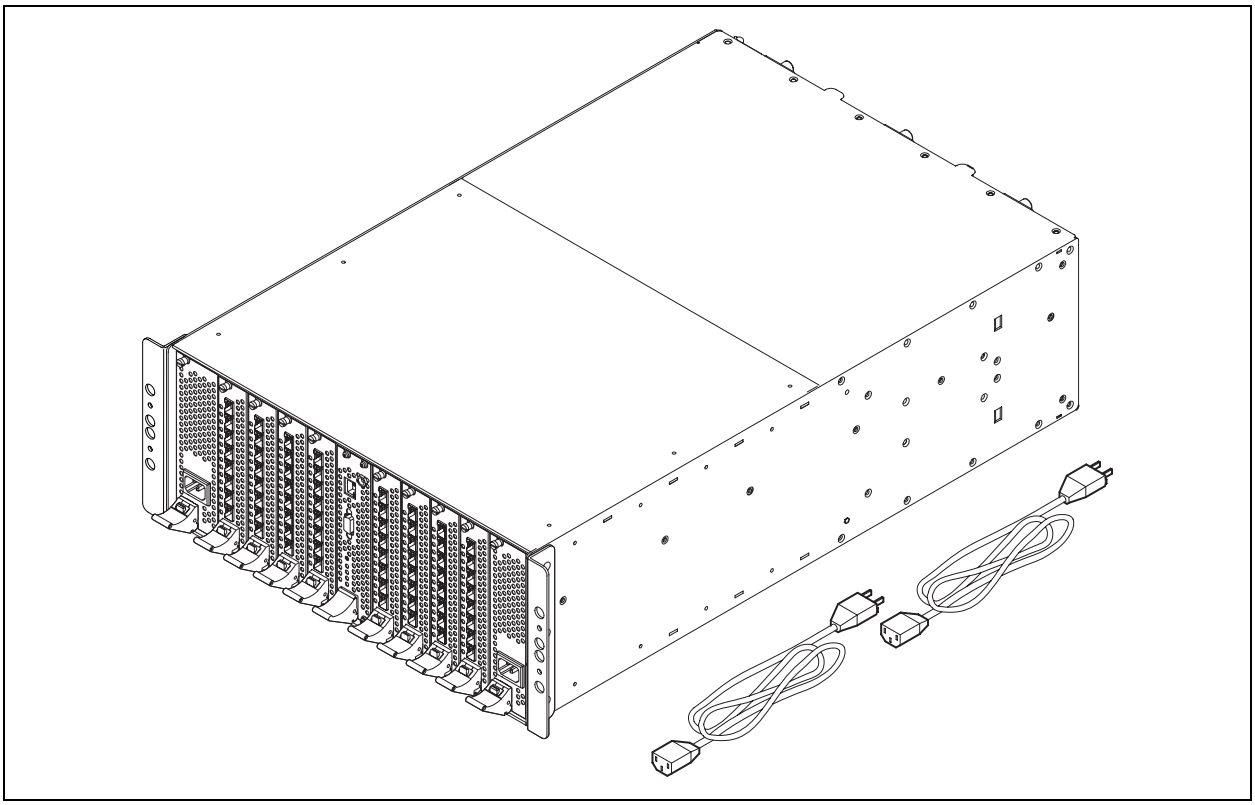


Figure 4-1. SANbox2-64 Fibre Channel Switch

Installing a SANbox2-64 switch involves the following steps:

1. Mount the switch.
2. Install SFP transceivers.
3. Connect the switch to the AC power source.
4. Connect the management workstation to the switch.
5. Install SANbox Manager.
6. Configure the switch.
7. Configure the ports.
8. Cable devices to the switch.

4.2.1 Mount the Switch

WARNING!! Two people are required to safely lift and install the SANbox2-64 switch into a rack. To avoid personal injury or damage to the switch, arrange for the help of an assistant.

When mounting products into a rack or cabinet, heavier products should be placed near the bottom. A top heavy rack can become unstable possibly resulting in equipment damage or personal injury.

CAUTION! If the switch is mounted in a closed or multi-unit rack assembly, make sure that the operating temperature inside the rack enclosure does not exceed the maximum rated ambient temperature. Refer to ”Environmental” on page A-4.

The switch must rest on rails or a shelf in the rack or cabinet. Allow 16 cm (6.5 in) minimum clearance at the front and rear of the rack for service access and ventilation.

Do not restrict chassis air flow. Allow 16 cm (6.5 in) minimum clearance at the front and rear of the rack for service access and ventilation.

Multiple rack-mounted units connected to the AC supply circuit may overload that circuit or overload the AC supply wiring. Consider the power source capacity and the total power usage of all switches on the circuit. Refer to ”Electrical” on page A-3.

Reliable grounding in the rack must be maintained from the switch chassis to the AC power source.

The switch is designed to be mounted in a rack using the mounting brackets and the SANbox2-64 rail kit shown in Figure 4-2. To mount the switch in a rack, do the following. Rack mounting instructions can also be found in the SANbox2-64 *Rack Mounting Guide* packaged with the switch.

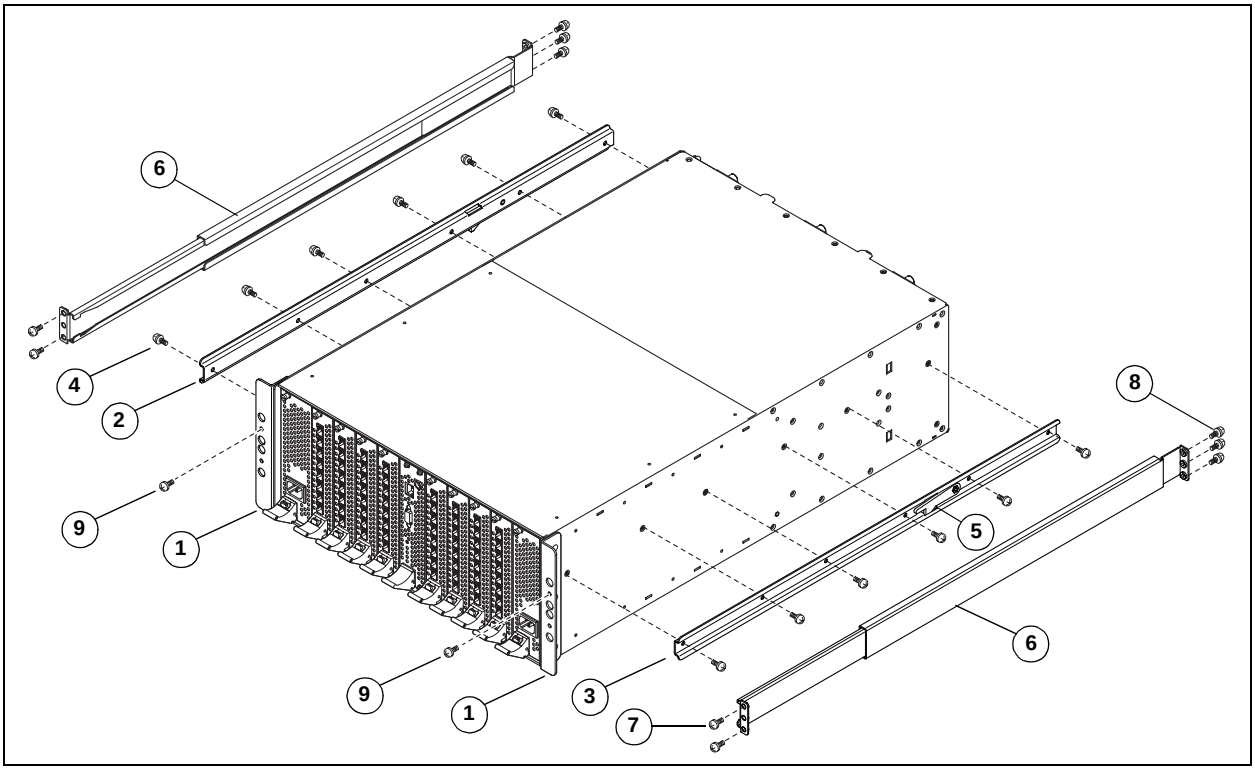


Figure 4-2. SANbox2-64 Rail Kit

1. You can install the switch in a rack “fans first” or “faceplate first”. The switch comes with two brackets (1) fastened to the front of the switch for a fans-first installation. These instructions assume a fans-first installation. To install the switch in the rack faceplate first, remove the mounting brackets and reinstall them on the rear corners of the switch.
2. Install left (2) and right (3) switch rails on the switch using six 8-32 screws (4) for each. Be sure that the latch is closest to the end of the switch that will be installed first in the rack and that the latch tab (5) is pointing down.
3. Extend the rack rails (6) to fit the inner dimensions of the rack. The rail flanges on both ends fit inside the rack. Be sure that the inner rail is toward the front. Fasten the front rail flange to the rack with two 10-32 screws (7) using the upper and lower holes. Fasten the rear end of the rail to the rack with three 10-32 screws (8).
4. Slide the switch and rail assembly into the rack rails. Fasten the switch to the rack with two screws (9), one through each bracket.

4.2.2
Install SFP Transceivers

The switch will support a variety of interconnection media. Refer to ”SFP Transceivers” on page 6-1 for information about removing and installing SFP transceivers.

4.2.3
Connect the Switch to AC Power

WARNING!! This product is supplied with a 3-wire power cable and plug for the user’s safety. Use this power cable in conjunction with a properly grounded outlet to avoid electrical shock. An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the switch chassis. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent electrical shock.

You may require a different power cable in some countries because the plug on the cable supplied with the equipment will not fit your electrical outlet. In this case, you must supply your own power cable. The cable you use must meet the following requirements: For 125 Volt electrical service, the cable must be rated at 13 Amps and be approved by UL and CSA. For 250 Volt electrical service: The cable must be rated at 13 Amps, meet the requirements of H05VV-F, and be approved by VDE, SEMKO, and DEMKO.

AVERTISSEMENT!!

Pour la sécurité de l’utilisateur, l’appareil est livré avec un câble d’alimentation trifilaire et une fiche. Pour éviter toute secousse électrique, enficher ce câble à une prise correctement mise à la terre.Une prise électrique dont les fils sont mal branchés peut créer une tension dangereuse dans les pièces métalliques du châssis switch. Pour éviter toute secousse électrique, s’assurer que les fils sont correctement branchés et que la prise est bien mise à la terre.

Dans certains pays les prises électriques sont de modèle différent; on ne peut y enficher le câble de l’appareil. On doit donc en utiliser un autre ayant les caractéristiques suivantes: Alimentation 125 V: Câble pour courant nominal de 10 A, agréé LAC et CSA. Alimentation 250 V: Câble pour courant nominal de 10 A, conforme au H05VV-F, et agréé VDE, SEMKO et DEMKO.

WARNUNG!!

Dieses Produkt wird mit einem 3-adrigen Netzkabel mit Stecker geliefert. Dieses Kabel erfüllt die Sicherheitsanforderungen und sollte an einer vorschriftsmäßigen Schukosteckdose angeschlossen werden, um die Gefahr eines elektrischen Schlages zu vermeiden.Elektrosteckdosen, die nicht richtig verdrahtet sind, können gefährliche Hochspannung an den Metallteilen des switch-Gehäuses verursachen. Der Kunde trägt die Verantwortung für eine vorschriftsmäßige Verdrahtung und Erdung der Steckdose zur Vermeidung eines elektrischen Schlages.

In manchen Ländern ist eventuell die Verwendung eines anderen Kabels erforderlich, da der Stecker des mitgelieferten Kabels nicht in die landesüblichen Steckdosen paßt. In diesem Fall müssen Sie sich ein Kabel besorgen, daß die folgenden Anforderungen erfüllt: Für 125 Volt-Netze: 13 Ampere Kabel mit UL- und CSA-Zulassung. Für 250 Volt-Netze: 13 Ampere Kabel gemäß den Anforderungen der H05VV-F und VDE-, SEMKO- und DEMKO-Zulassung.

To connect the switch to an AC power source and energize the switch, do the following:

1. Connect the power cords to the AC power receptacles on the front of the switch chassis.
2. Connect each power cord to a 3-wire, grounded, AC outlet that delivers power in accordance with the power requirements in Appendix A Specifications.

Note: To provide redundancy in the event of an AC power circuit failure, connect the switch power supplies to separate AC circuits.

3. As the switch powers up, the chassis LEDs mark the process with the following sequence:
   a. All chassis LEDs illuminate briefly as the BIOS starts.
   b. When the BIOS is complete, the Input Power LED remains illuminated while the other LEDs are extinguished.
   c. After about a minute, all LEDs illuminate again when the switch Power-on Self Test (POST) completes. The POST tests the condition of firmware, memories, data-paths, and switch logic circuitry.

d. About 10 seconds later, the switch is operational: the Input Power LED remains illuminated, the Heartbeat LED flashes steadily, and the two remaining LEDs are extinguished. If the Heartbeat LED blinks steadily about once per second, the POST was successful and you can continue with the installation process. Any other blink pattern indicates that an error has occurred. Refer to "Heartbeat LED Blink Patterns" on page 5-1 for more information about the error blink pattern.

4. Confirm that the Output Power LEDs on both power supplies are illuminated. If not, check the power cords and the AC voltage source. Refer to "Output Power LED Is Extinguished" on page 5-11 for more information about troubleshooting procedures.

4.2.4
Connect the Management Workstation to the Switch

Connect the management workstation to the switch in one of three ways:

- Indirect Ethernet connection from the management workstation to the switch RJ-45 Ethernet connector through an Ethernet switch or a hub. This requires a 10/100 Base-T straight cable as shown in Figure 4-3. With this method, you can manage the switch with SANbox Manager or the CLI.
- Direct Ethernet connection from the management workstation to the switch RJ-45 Ethernet connector. This requires a 10/100 Base-T cross-over cable as shown in Figure 4-3. With this method, you can manage the switch with the SANbox Manager application or the CLI.
- Serial port connection from the management workstation to the switch RS-232 connector. This requires a null modem F/F DB9 cable as shown in Figure 4-3. With this method, you can manage the switch with the CLI.

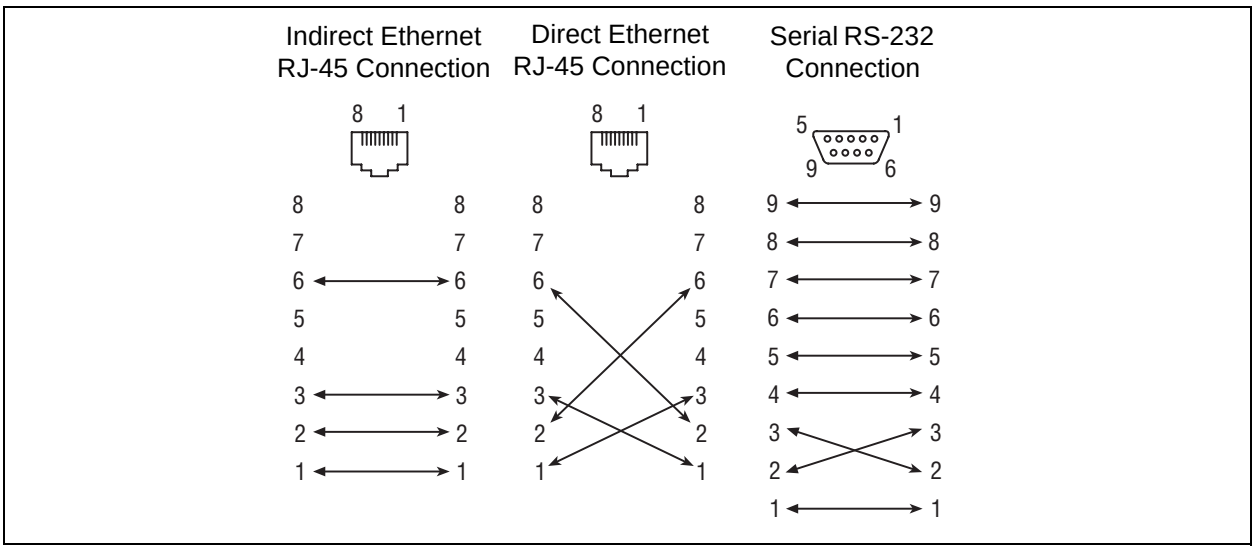


Figure 4-3. Ethernet and Serial Cable Connections

4.2.4.1
Ethernet Connection

To establish an Ethernet connection, do the following:

1. Connect a 10/100 Base-T cross-over cable from an RJ-45 port on the management workstation directly to the RJ-45 Ethernet port; or a 10/100 Base-T straight cable indirectly over an Ethernet network.
2. Open a command line window.
3. Open a Telnet session by entering the following command with the switch IP address. The default IP address is 10.0.0.1

```
telnet 10.0.0.1
```

4. Log in to the switch. If fabric security is disabled, account names and passwords are not enforced. Refer to the "Set Setup Command" on page B-40 for information about setting fabric security. The default account name and password are (admin, password).

```
SANbox2 Login: admin
Password: ********
```

4.2.4.2
Serial Connection

To establish a serial port connection, do the following:

1. Connect a null modem F/F DB9 cable from a COM port on the management workstation to the RS-232 serial port on the switch.
2. Configure the connection according to your platform:
   - For Windows:
     a. Open the HyperTerminal application on a Windows platform. Choose the **Start** button, select **Programs, Accessories, HyperTerminal,** and **HyperTerminal**.
     b. Enter a name for the switch connection and choose an icon in the Connection Description window. Choose the **OK** button.
     c. Select the COM port in the Connect To window and choose the **OK** button.
     d. Enter the following COM Port settings in the COM Properties window and choose the **OK** button.
        - ❑ Bits per second: 9600
        - ❑ Data Bits: 8
        - ❑ Parity: None
        - ❑ Stop Bits: 1
        - ❑ Flow Control: None

- For Linux:
  a. Set up minicom to use the serial port. Create or modify the /etc/minirc.dfl file with the following content:

```
pr portdev/ttyS0
pu minit
pu mreset
pu mhangup
```

  b. Verify that all users have permission to run minicom. Review the /etc/minicom/users file and confirm that the line "ALL" exists or that there are specific user entries.
  c. Enter the following command at the Linux prompt:

```
minicom
```

- For Solaris:
  a. Set up Solaris to use the serial port. Modify the /etc/remote file to include the following lines:

```
sanbox2:\
:dv=/dev/term/a:br#9600:el=C^S^Q^U^D:ie%$:oe=^D:
```

  b. Enter the following command at the Solaris prompt:

```
# tip sanbox2
```

3. Log in to the switch. If fabric security is disabled, account names and passwords are not enforced. Refer to the "Set Setup Command" on page B-40 for information about setting fabric security. The default account name and password are (admin, password).

```
SANbox2 Login: admin
Password: ********
```

4.2.5 Installing SANbox Manager

You can install SANbox Manager on the Windows, Linux, and Solaris platforms. Your switch was shipped with either a SANsurfer® Management Suite Disk or a SANbox2 Installation Disk. Refer to the following installation instructions that correspond to your situation:

- SANsurfer Management Suite Disk - Windows Installation
- SANsurfer Management Suite Disk - Linux Installation
- SANsurfer Management Suite Disk - Solaris Installation
- SANbox2 Installation Disk - Windows Installation
- SANbox2 Installation Disk - Linux Installation
- SANbox2 Installation Disk - Solaris Installation

4.2.6
SANsurfer Management Suite Disk - Windows Installation

To install the SANbox Manager application on Windows from the SANsurfer® Management Suite Disk, do the following:

1. Close all programs currently running, and Insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If the SANsurfer Management Suite start page does not open in your default browser, do the following:
   a. Using Windows Explorer, double-click the drive letter which contains the SANsurfer Management Suite Disk.
   b. Locate and double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page in your default browser.
2. On the SANsurfer Management Suite start page, choose the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 (2Gb) Series area.
4. In the Windows column, choose the **SANbox Manager** link to open the File Download window.
5. You have a choice of running the installation file from the CD-ROM or downloading the installation file to your hard drive. Choose one of the following:
   - Open the installation file from the CD-ROM and follow the SANbox Manager installation instructions.
   - Specify a location in which to save the **sansurfer_windows_install.exe** file, and choose the **Save** button. Double-click the saved **sansurfer_windows_install.exe** file and follow the SANbox Manager installation instructions.

4.2.7
SANsurfer Management Suite Disk - Linux Installation

To install the SANbox Manager application on Linux from the SANsurfer Management Suite Disk, do the following:

1. Close all programs currently running, and insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If a file browser window opens showing icons for the contents of the CD-ROM, double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page. If a file browser does not open, double-click the CD-ROM icon on the to open the browser. If there is no CD-ROM icon, do the following:
   a. Open an xterm or other terminal window.
   b. Mount the CD-ROM. From a shell prompt, enter the following command:

      ```
      mount /mnt/cdrom
      ```

   c. Execute your web browser to view the **Start_Here.htm** document using one of the following commands:

      ```
      $mozilla file:/mnt/cdrom/Start_Here.htm
      ```

      or

      ```
      $netscape file:/mnt/cdrom/Start_Here.htm
      ```

   d. The SANsurfer Management Suite start page opens in your default browser.
2. On the SANsurfer Management Suite start page, choose the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 (2Gb) Series area.
4. In the Linux column, choose the **SANbox Manager** link to open the Save As window.
5. Enter a path name to save the **sansurfer_linux_install.bin** file, and choose the **Save** button.
6. Open a terminal window for the directory in which the **sansurfer_linux_install.bin** file was saved, and enter the following command and press the **Enter** key:

   ```
   chmod +x sansurfer_linux_install.bin
   ```

7. Enter the following command:

   ```
   ./sansurfer_linux_install.bin
   ```

8. Press the **Enter** key, and follow the SANbox Manager installation instructions.

4.2.8
SANsurfer Management Suite Disk - Solaris Installation

To install the SANbox Manager application on Solaris from the SANsurfer Management Suite CD-ROM, do the following:

1. Close all programs currently running, and insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If the SANsurfer Management Suite start page does not open in your default browser, do the following:
   a. Right-click the to open the Workshops Menu.
   b. Point to and select **Files**, then select **File Manager**.
   c. In File Manager, double-click the CD-ROM icon, and then double-click the Sansurfer folder.
   d. In the Sansurfer folder, double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page in your default browser.
2. On the SANsurfer Management Suite start page, choose the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 (2Gb) Series area.
4. In the Solaris column, choose the **SANbox Manager** link to open the Save As window.
5. Enter a path name to save the **sansurfer_solaris_install.pkg** file and choose the **Save** button.
6. Open a terminal window for the directory in which the **sansurfer_solaris_install.pkg** file was saved, and enter the following command:

   ```
   chmod +x sansurfer_solaris_install.pkg
   ```

7. Press the **Enter** key.
8. Enter the following command:

   ```
   ./sansurfer_solaris_install.pkg
   ```

9. Press the **Enter** key, and follow the SANbox Manager installation instructions.

Note: If you download SANbox Manager from a server, be sure the downloaded file has execute permission before installing.

4.2.9
SANbox2 Installation Disk - Windows Installation

To install the SANbox Manager application on Windows from the SANbox2 Installation Disk, do the following:

1. Close all programs currently running, and insert the SANbox2 Installation Disk into the management workstation CD-ROM drive.
2. Using Windows Explorer, double-click the drive letter which contains the SANbox2 Installation Disk.
3. Double click the SANbox_Manager folder, then double click the Windows folder.
4. Double click the executable file and follow the SANbox Manager installation instructions.

4.2.10
SANbox2 Installation Disk - Linux Installation

To install the SANbox Manager application on Linux from the SANbox2 Installation Disk, do the following:

1. Close all programs currently running, and insert the SANbox2 Installation Disk into the management workstation CD-ROM drive.
2. Open the File Manager and double-click on the CD-ROM icon.
3. Double click the SANbox_Manager folder, then double click the Linux folder.
4. Double click the executable file and follow the SANbox Manager installation instructions.

4.2.11
SANbox2 Installation Disk - Solaris Installation

To install the SANbox Manager application on Solaris from the SANbox2 Installation Disk, do the following:

1. Close all programs currently running, and insert the SANbox2 Installation Disk into the management workstation CD-ROM drive.
2. Open a terminal window. If the disk isn't already mounted, enter the following command:

   ```
   mount /mnt/cdrom
   ```

3. Move the directory on the disk that contains the executable. Enter the following command:

   ```
   cd cdrom/cdrom0/sanbox~1/solaris
   ```

4. Run the executable and follow the SANbox Manager installation instructions. Enter the following command:

   ```
   pkgadd -d sol_pkg
   ```

4.2.12
Configure the Switch

Do the following to configure a switch using the SANbox Manager application. Refer to the *SANbox2-64 Switch Management User's Guide* for more information about configuring a switch. You can also configure the switch using the CLI. Refer to Appendix B Command Line Interface for more information.

1. Connect to the switch using an Ethernet connection and run SANbox Manager.
2. Open the Fabric menu and select **Add Fabric** to open the Add a New Fabric window.
3. Enter a fabric name and the IP address of the switch through which to manage the fabric. The default IP address is 10.0.0.1. If this is a new switch, leave the login name and password fields empty, and choose the **Add Fabric** button. By default, fabric security is disabled, and therefore account names and passwords are not enforced. Refer to the "Set Setup Command" on page B-40 for information about setting fabric security.
4. Open the Switch menu and select **Switch Properties**. In the Switch Properties window, enter a chassis name. Accept the default domain ID, and choose the **OK** button.

5. Open the Switch menu and select **Network Properties**. In the Network Properties window, enter values for the IP address, subnet mask, and gateway address. Accept the default boot method. If you know the SNMP configuration settings, enter those as well. Choose the **OK** button.
6. Set the date and time. Double click on the switch in the topology display. In the faceplate display, open the Switch menu and select **Set Date/Time**. Enter the date and time in the Switch Date and Time window and choose the **OK** button. Reset the switch when prompted to implement the new and date and time.

Repeat this process for each switch in the fabric, then connect the switches.

4.2.13
Configure the Ports

Configuring a port involves defining the port mode. For public devices and other switches, a switch automatically sets the port mode as each port discovers the type of device to which it is connected.

A GL_Port will self configure as an FL_Port when connected to a loop of public devices or an F_Port when connected to a single device. A G_Port will self configure as an F_Port when connected to a single public device. Both GL_Ports and G_Ports self configure as E_Ports when connected to another switch. The default port mode is GL_Port. Refer to the *SANbox2-64 Switch Management User's Guide* for more information about configuring ports. You can also configure ports using the CLI. Refer to Appendix B Command Line Interface for information about the command line interface.

4.2.14
Cable Devices to the Switch

Connect cables to the SFP transceivers and their corresponding devices, and then energize the devices. Device host bus adapters can have SFP (or SFF) transceivers or GigaBit Interface Converters (GBIC). LC-type duplex fiber optic cable connectors are designed for SFP transceivers, while SC-type connectors are designed for GBICs. Duplex cable connectors are keyed to ensure proper orientation. Choose the fiber optic cable with the connector combination that matches the device host bus adapter.

4.3 Install Firmware

The switch comes with current firmware installed. You can upgrade the firmware from the management workstation as new firmware becomes available. Firmware installation involves loading the firmware image file onto the switch, unpacking the image file, and then resetting the switch to activate the new firmware. New firmware can be loaded on the switch while the switch is operating without disrupting service. However, you must reset the switch to activate the new firmware, which does disrupt service.

You can use the SANbox Manager application or the CLI to install new firmware:

- The SANbox Manager application loads and unpacks the firmware image file in one operation. Refer to ”Using SANbox Manager to Install Firmware” on page 4-16.
- When using the CLI on a workstation that has an FTP server, you can open a Telnet session and load and unpack the firmware image file using the CLI Image command. Refer to ”Using the CLI to Install Firmware” on page 4-17.
- When using the CLI on a workstation without an FTP server, you must open an FTP session through the switch to load the image file, then open a Telnet session to unpack it with the CLI Image command. Refer to ”Using FTP and the CLI to Install Firmware” on page 4-18.

4.3.1 Using SANbox Manager to Install Firmware

To install firmware using SANbox Manager, do the following:

1. From the Faceplate display, open the Switch menu and select **Load Firmware**.
2. In the Firmware Upload window, browse and select the firmware file you want to load.
3. In the Firmware Upload window, choose the **Start** button to begin the loading process. When the firmware is finished loading, the Bytes Transferred field displays the number of bytes that have been transferred.
4. Choose the **Close** button to close the Firmware Upload window.
5. Open the Switch menu and select **Reset Switch** to activate the new firmware.

4.3.2
Using the CLI to Install Firmware

To install firmware using the CLI when an FTP server is present on the management workstation, do the following:

1. Connect to the switch through the Ethernet or the serial port and open a Telnet session.
2. Enter the following account name and password:

   ```
   SANbox2 Login:admin
   Password: password
   ```

3. To start an admin session, enter the following:

   ```
   cli $> admin start
   ```

4. Retrieve the firmware file. The device on which the firmware file is stored must be running an FTP server. Enter the following command to retrieve the firmware file from the specified IP address:

   ```
   cli (admin) #> image fetch username 10.0.0.254
   firmwarefilenametoload firmwarefilenameonswitch
   Connected to 10.0.0.254.
   ```

   Note: If prompted for your password, enter your password (for that IP Address) and press the Enter key.

   ```
   331 Password required for username.
   Password:
   230 User username logged in.
   bin
   200 Type set to I.
   verbose
   Verbose mode off.
   ```

5. Enter the following command to display the list of firmware files:

   ```
   cli (admin) #> image listfirmwarefilenameonswitch
   ```

6. Enter the following command to install the new firmware:

   ```
   cli (admin) #>image unpack firmwarefilenameonswitch
   ```

7. Reset the switch to activate the new firmware.

   ```
   cli (admin) $>reset
   ```

4.3.3
Using FTP and the CLI to Install Firmware

To install firmware using the CLI when the management workstation does not have an FTP server, do the following:

1. Connect to the switch through the Ethernet or the serial port.
2. Move to the folder or directory that contains the new firmware image file.
3. Establish communications with the switch using the File Transfer Protocol (FTP). Enter one of the following on the command line:

   `>ftp xxx.xxx.xxx.xxx`

   or

   `>ftp switchname`

   where *xxx.xxx.xxx.xxx* is the switch IP address, and *switchname* is the switch name associated with the IP address.
4. Enter the following account name and password:

   `user:images`

   `password: images`
5. Activate binary mode and copy the firmware image file on the switch:

   `ftp>bin`

   `ftp>put filename`
6. Close the FTP session.

   `ftp>quit`
7. Establish communications with the switch using the CLI. Enter one of the following on the command line:

   `telnet xxx.xxx.xxx.xxx`

   or

   `telnet switchname`

   where *xxx.xxx.xxx.xxx* is the switch IP address, and *switchname* is the switch name associated with the IP address.
8. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are (admin, password).
9. Open an Admin session to acquire the necessary authority.

   `cli $>admin start`

10. Display the list of firmware image files on the switch to confirm that the file was loaded. Refer to the ”Image Command” on page B-15 for more information.

```
cli (admin) $>image list
```

11. Unpack the firmware image file to install the new firmware in flash memory.

```
cli (admin) $>image unpack filename
```

12. Reset the switch to activate the new firmware. This will close the Telnet session by default.

```
cli (admin) $>reset
```

4.4 Powering Down a Switch

Simply unplugging the switch from the power source does not allow the switch to complete executing tasks and could lead to flash memory corruption. For this reason, open a Telnet session and use the Shutdown command to initiate an orderly shut down, then power down the switch. Refer to the ”Shutdown Command” on page B-65.

Notes

Section 5

Diagnostics/Troubleshooting

Diagnostic information about the switch is available through the chassis LEDs, the power supply LEDs, and the Port Status LED. Diagnostic information is also available through the SANbox Manager and CLI event logs and error displays. This section describes two types of diagnostics: Power On Self Test (POST) and chassis. POST diagnostics describe the Heartbeat LED and the Port Status LED indications. Chassis diagnostics cover power supply and fan diagnostics as well as over temperature conditions. This section also describes how to use maintenance mode to recover a disabled switch.

5.1
POST Diagnostics

The switch performs a series of Power On Self Tests (POST) as part of its power-up procedure. The POST diagnostic program performs the following tests:

- Checksum tests on the boot firmware in PROM and the switch firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the ASIC

During the POST, the switch logs any errors encountered. Some POST errors are fatal, others are non-fatal. The switch uses the Heartbeat LED and the Port Status LED to indicate switch and port status. A fatal error disables the switch so that it will not operate. A non-fatal error allows the switch to operate, but disables the ports that have errors. Whether the problem is fatal or non-fatal, contact your authorized maintenance provider.

If there are no errors, the Heartbeat LED blinks at a steady rate of once per second. If a fatal error occurs, the Heartbeat LED will show an error blink pattern. If there are non-fatal errors, the switch disables the failed ports and flashes the associated Port Status LEDs. Refer to ”Heartbeat LED Blink Patterns” on page 5-1 for more information about Heartbeat LED blink patterns.

5.1.1
Heartbeat LED Blink Patterns

5.1.1.1
Normal (all pass)

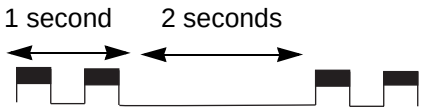
If all POST diagnostics pass, the switch will go to normal operation and the Heartbeat LED will blink at a steady rate of one (1) blink per second.

5.1.1.2
Maintenance Mode Pattern

Steady illumination indicates that the switch is in maintenance mode, which returns the switch IP address to 10.0.0.1. From maintenance mode, you may reload firmware, reset the password to the factory default, and remove a corrupt configuration.

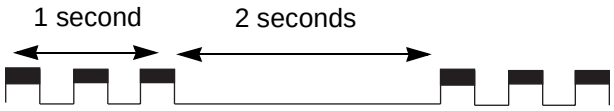
5.1.1.3
Internal Firmware Failure Blink Pattern

An internal firmware failure blink pattern is 2 blinks per second followed by a two second pause. The 2-blink error pattern indicates that the firmware has failed, and that the switch must be reset. Press and release the Maintenance button to reset the switch.



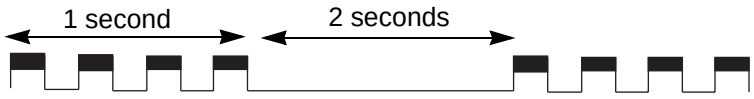
5.1.1.4
Fatal Error Blink Pattern

A fatal error blink pattern is 3 blinks per second followed by a two second pause. The 3-blink error pattern indicates that a fatal error has left the switch inoperable. If a fatal error occurs, contact your authorized maintenance provider.



5.1.1.5
Configuration File System Error Blink Pattern

A configuration file system error blink pattern is 4 blinks per second followed by a two second pause. The 4-blink error pattern indicates that a configuration file system error has occurred, and that the configuration file must be recreated.



To recreate the configuration file, do the following:

1. Open a Telnet session and use the Shutdown command to close activity on the switch, then power down the switch. Refer to the ”Shutdown Command” on page B-65.

2. Place the switch in maintenance mode. Press and hold the Maintenance button for about 4 seconds. Refer to "Recovering a Switch" on page 5-12 for more information about placing the switch in maintenance mode.
3. Establish a Telnet session with the switch using the default IP address 10.0.0.1.

```
telnet 10.0.0.1
```

4. Enter the account name (prom) and password (prom), and press the Enter key.

```
Sanbox2 login: prom
Password:xxxx
[username@host:Itasca]% telnet 10.0.0.1
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
```

5. The following menu is displayed. Enter "6" (Remake Filesystem) and press the Enter key to recreate the configuration file.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset Password File
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
Option: 6
```

6. When the recreate process is complete, select option 7 to reset the switch and exit maintenance mode.
7. If a previously saved configuration file is available for the switch, do the following to restore the configuration file.
   a. Establish communications with the switch using the File Transfer Protocol (FTP). Enter one of the following on the command line:

      `>ftp` *`xxx.xxx.xxx.xxx`*

      or

      `>ftp` *`switchname`*

      where *xxx.xxx.xxx.xxx* is the switch IP address and *switchname* is the switch name associated with the IP address.

   b. Enter the following account name and password:

      `user:`*`images`*

      `password:`*`images`*

c. Activate binary mode and copy the configuration file from the workstation to the switch. The configuration file must be named "configdata".

```
ftp>bin
ftp>put configdata
```

d. Close the FTP session.

```
ftp>quit
```

e. Establish communications with the switch using Telnet. Enter one of the following on the command line:

`telnet` *`xxx.xxx.xxx.xxx`*

or

`telnet` *`switchname`*

where *xxx.xxx.xxx.xxx* is the switch IP address and *switchname* is the switch name associated with the IP address.

f. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are (admin, password).

g. Open an admin session to acquire the necessary authority.

```
cli $>admin start
```

h. Restore the configuration file.

```
cli (admin) $>config restore
```

i. Reset the switch and close the Telnet session.

```
cli (admin) $>reset
```

5.1.2

Port Status LED Indications

Port diagnostics for each port are indicated by the Port Status LED as shown in Figure 5-1.

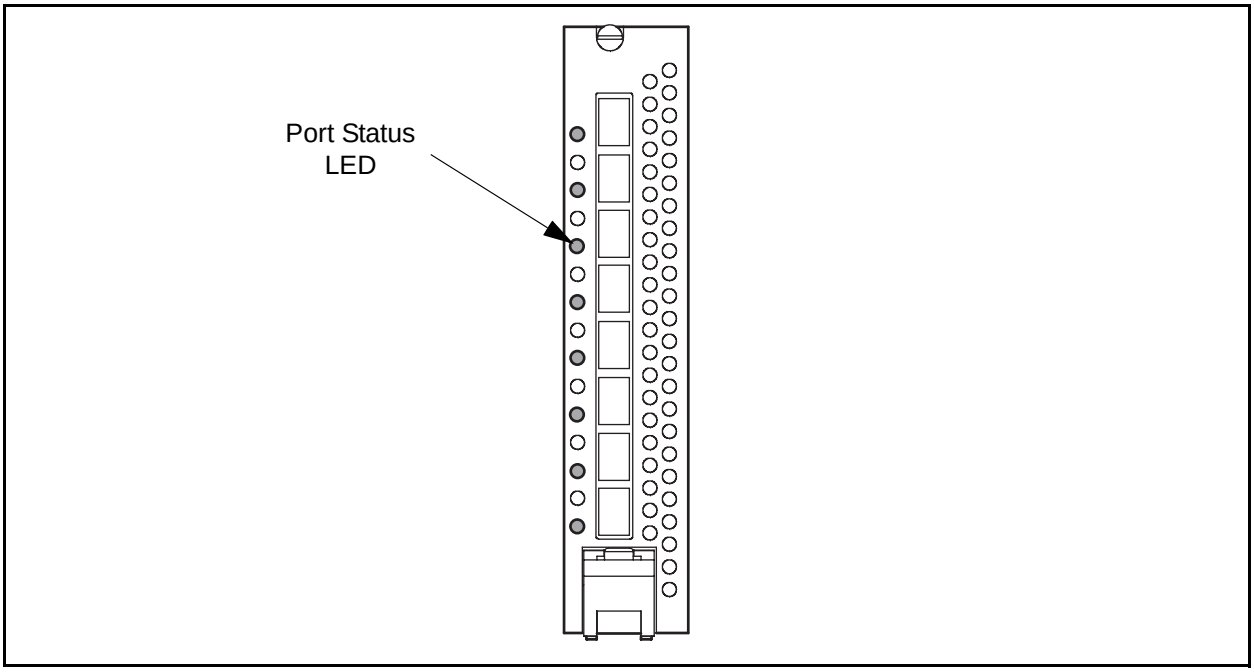


Figure 5-1. Port Status LED

The Port Status LED has three indications:

- Logged in - Continuous illumination.
- Logging in - Flashes at roughly once per second as shown in Figure 5-2.
- Error - Flashes at roughly twice per second as shown in Figure 5-2.

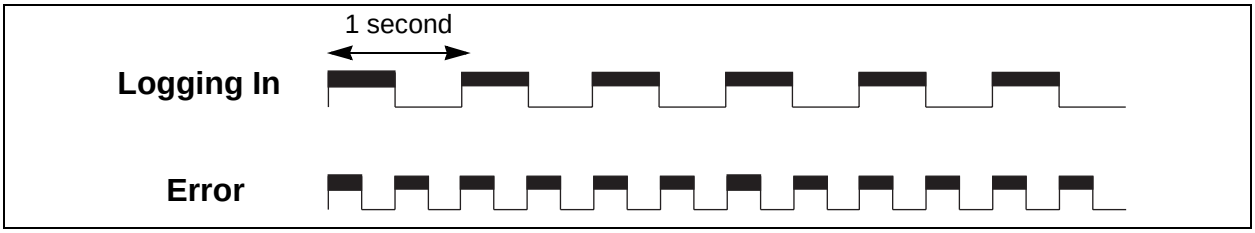


Figure 5-2. Port Status LED Indications

If a Port Status LED shows an error indication, review the alarm log for messages regarding the affected port. You can inspect the alarm log using the Alarm data tab in SANbox Manager faceplate display or the Show Alarm command. Pertinent alarm log messages will point to one or more of the following conditions:

- E_Port isolation
- Excessive port errors

5.1.2.1

E_Port Isolation

A Port Status LED error indication is often the result of E_Port isolation. An isolated E_Port is indicated by a red link in the SANbox Manager topology display. E_Port isolation can be caused by conflicting domain IDs, conflicting timeout values, or conflicting zone membership between active zone sets. Refer to the *SANbox2-64 Switch Management User's Guide* for information about how to change domain IDs, timeout values, and edit zoning.

Review the alarm log and do the following to diagnose and correct an isolated E_Port:

1. Display the fabric domain IDs using the Show Domains command or the Switch data tab in the SANbox Manager topology display. Are all domain IDs in the fabric unique?
   - Yes - Continue.
   - No - Correct the domain IDs on the offending switches using the Set Config Switch command or the SANbox Manager Switch Properties window. Reset the port. If the condition remains, continue.
2. Compare the RA_TOV, ED_TOV, RT_TOV timeout values for all switches in the fabric using the Show Config Switch command or the Switch data tab of the SANbox Manager topology display. Is each timeout value the same on every switch?
   - Yes - Continue.
   - No - Correct the timeout values on the offending switches using the Set Config Switch command or the SANbox Manager Switch Properties window. Reset the port. If the condition remains, continue.

3. Display the active zone set on each switch using the Zoning Active command or the Active Zoneset tab of the SANbox Manager topology display. Compare the zone membership between the two active zone sets. Are they the same?
   - Yes - Contact your authorized maintenance provider.
   - No - Deactivate one of the active zone sets or edit the conflicting zones so that their membership is the same. Reset the port. If the condition remains, contact your authorized maintenance provider.

     Note: This can be caused by merging two fabrics whose active zone sets have two zones with the same name, but different membership.

5.1.2.2

Excessive Port Errors

The switch monitors a set of port errors and generates alarms based on user-defined sample intervals and thresholds. Refer to the *SANbox2-64 Switch Management User's Guide* for information about managing alarms. These port errors include the following:

- CRC errors
- Decode errors
- ISL connection count
- Login errors
- Logout errors
- Loss-of-signal errors

If the count for any of these errors exceeds the rising threshold for three consecutive sample intervals, the switch generates an alarm and disables the affected port, changing its operational state to "down". Port errors can be caused by the following:

- Thresholds are too low or the sample interval is too small
- Faulty Fibre Channel port cable
- Faulty SFP
- Faulty port
- Fault device or HBA

Review the alarm log to determine if excessive port errors are responsible for disabling the port. Look for a message that mentions one of the monitored error types indicating that the port has been disabled, then do the following:

1. Examine the alarm configuration for the associated error using the Show Config Threshold command or the SANbox Manager application. Refer to the "Show Config Command" on page B-55. Refer to Table B-4 for a list of the alarm configuration defaults. Are the thresholds and sample interval correct?
   - Yes - Continue
   - No - Correct the alarm configuration. If the condition remains, continue.
2. Reset the port, then perform an external port loopback test to validate the port and the SFP. Refer to the "Test Command" on page B-66 or the *SANbox2-64 Switch Management User's Guide* for information about testing ports. Does the port pass the test?
   - Yes - Continue
   - No - Replace the SFP and repeat the test. If the port does not pass the test, contact your authorized maintenance provider. Otherwise continue.
3. Replace the Fibre Channel port cable. Is the problem corrected?
   - Yes - Complete.
   - No - Continue.
4. Inspect the device to which the affected port is connected and confirm that the device and its HBA are working properly. Make repairs and corrections as needed. If the condition remains, contact your authorized maintenance provider.

5.2

Chassis Diagnostics

Chassis diagnostics are indicated by the chassis and power supply LEDs as shown in Figure 5-3.

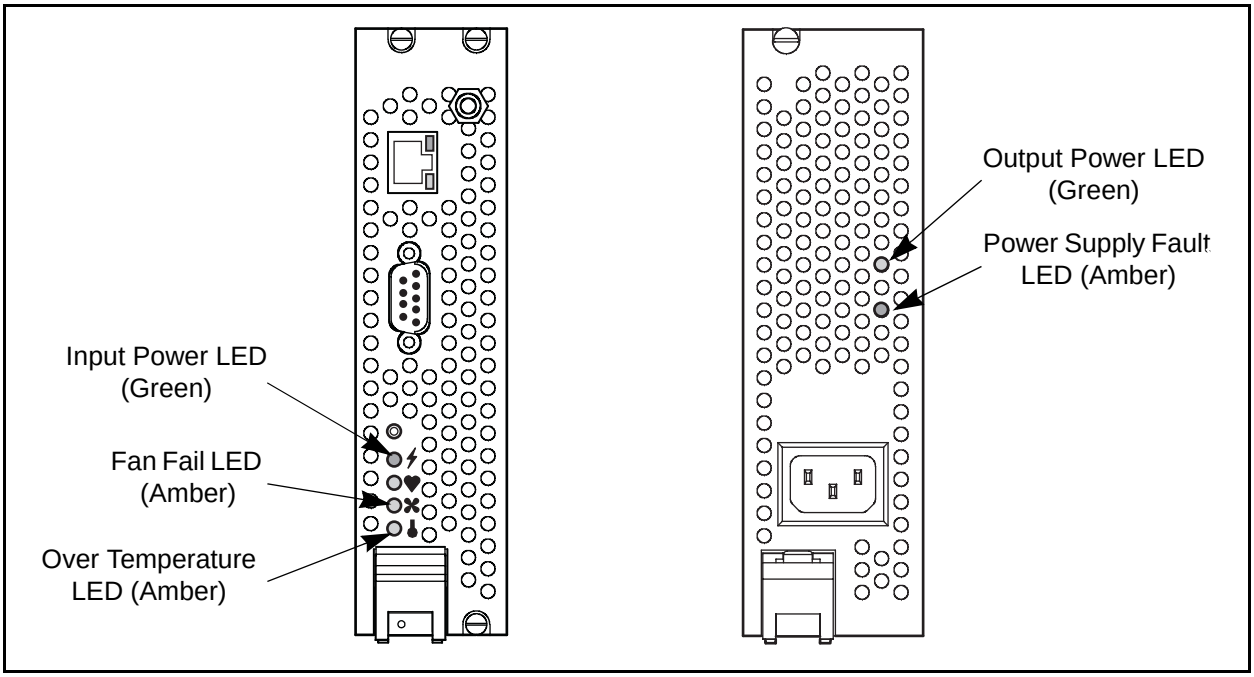


Figure 5-3. Chassis and Power Supply LEDs

The following conditions are described:

- Over Temperature LED is illuminated
- Input Power LED is extinguished
- Fan Fail LED is illuminated
- Output Power LED is extinguished
- Power Supply Fault LED is illuminated

5.2.1
Over Temperature LED is Illuminated

The Over Temperature LED illuminates to indicate that the switch logic circuitry is overheating. If the Over Temperature LED illuminates, do the following:

1. Inspect the chassis fans. Are the intake openings clear? Are all fans operating and producing air flow?
   - Yes - Continue.
   - No - Remove any debris from fan intakes and exhausts if necessary. Replace any fan that is not operating. Refer to Section 6 Removal/Replacement. If the condition remains, continue.
2. Consider the ambient air temperature near the switch. Make necessary corrections. If the condition remains, shut down the switch immediately and contact your authorized maintenance provider.

5.2.2
Input Power LED Is Extinguished

The Input Power LED illuminates to indicate that the switch logic circuitry is receiving proper voltages. If the Input Power LED is extinguished, inspect the Output Power LED. Is the Output Power LED illuminated?

- Yes - Contact your authorized maintenance provider.
- No - Refer to ”Output Power LED Is Extinguished” on page 5-11.

5.2.3
Fan Fail LED is Illuminated

The Fan Fail LED illuminates to indicate a malfunction with one or more of the chassis fans. If the Fan Fail LED illuminates, do the following:

1. Inspect the chassis fan connections. Remove and reinstall the chassis fan. Refer to Section 6 Removal/Replacement. If the condition remains, continue.
2. Are all fans operating and producing equal air flow?
   - Yes - Contact your authorized maintenance provider.
   - No - Replace the weaker chassis fan. Refer to Section 6 Removal/Replacement. If the condition remains, contact your authorized maintenance provider.

Note: Removing a fan will not illuminate the Fan Fail LED.

5.2.4
Output Power LED Is Extinguished

The Output Power LED illuminates to indicate that the power supply is producing the proper voltages. If the Output Power LED is extinguished, do the following:

1. Inspect the Power Supply Fault LED. Is the Power Supply Fault LED illuminated?
   - Yes - Refer to ”Power Supply Fault LED is Illuminated” on page 5-11.
   - No - Continue.
2. Inspect the power cables and connectors. Are the cables unplugged? Are the cables or connectors damaged?
   - Yes - Make necessary corrections or repairs. If the condition remains, continue.
   - No - Continue.
3. Inspect the power source. Is the power source delivering the proper voltage?
   - Yes - Continue
   - No - Make necessary repairs. If the condition remains, continue.
4. Replace the power supply. Refer to Section 6 Removal/Replacement. If the condition remains, contact your authorized maintenance provider.

5.2.5
Power Supply Fault LED is Illuminated

The Power Supply Fault LED illuminates to indicate a power supply fault. Possible fault conditions include high temperature, high output voltage, or low output voltage. If the Power Supply Fault LED illuminates, do the following:

1. Inspect the chassis fans. Are the intake openings clear? Are all fans operating and producing air flow?
   - Yes - Continue.
   - No - Remove any debris from fan intakes if necessary. Replace any fan that is not operating. Refer to Section 6 Removal/Replacement. If the condition remains, continue.
2. Consider the ambient air temperature near the switch and clearance around the switch. Make necessary corrections. If the condition remains, continue.
3. Replace the power supply. Refer to Section 6 Removal/Replacement. If the condition remains, contact your authorized maintenance provider.

5.3
Recovering a Switch

A switch can become inoperable or unavailable for the following reasons:

- Firmware becomes corrupt
- IP address is lost
- Switch configuration becomes corrupt
- Forgotten password

In these specific cases, you can recover the switch using maintenance mode. Maintenance mode returns the switch IP address to 10.0.0.1 and provides opportunities to do the following:

- Unpack a firmware image file
- Restore the network configuration parameters to the default values
- Remove all user accounts and restore the Admin account name password to the default.
- Copy the log file
- Restore factory defaults for all but user accounts and zoning
- Restore all switch configuration parameters to the factory default values
- Reset the switch

To recover a switch, do the following:

1. Place the switch in maintenance mode. Do the following:
   a. Power down the switch.
   b. Press and hold the Maintenance button with a pointed tool, then power up the switch. All chassis LEDs will illuminate, then extinguish leaving only the Input Power LED illuminated. Release the button.
2. Allow one minute for the switch to complete its tests. When the switch is in maintenance mode, the Input LED will be illuminated and the Heartbeat LED will illuminate continuously. All other chassis LEDs will be extinguished.
3. Establish a Telnet session with the switch using the maintenance mode IP address 10.0.0.1.
4. Enter the maintenance mode account name and password (prom, prom), and press the Enter key.

```
Sanbox login: prom
Password:xxxx
[username@anteater:Itasca]% telnet 10.0.0.1
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
```

5. The maintenance menu displays several recovery options. To select a switch recovery option, press the corresponding number (displayed in option: field) on the keyboard and press the Enter key.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset Password File
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
Option:
```

These options and their use are described in the following sections.

5.3.1 Maintenance – Exit

This option closes the current login session. To log in again, enter the maintenance mode account name and password (prom, prom).

5.3.2 Maintenance – Image Unpack

This option unpacks and installs new firmware when the current firmware has become corrupt. Before using this option, you must load the new firmware image file onto the switch. The steps to install new firmware using this option are as follows:

1. Place the switch in maintenance mode. Refer to the procedure for maintenance mode in ”Recovering a Switch” on page 5-12.
2. Use FTP to load a new firmware image file onto the switch. Refer to ”Using FTP and the CLI to Install Firmware” on page 4-18. Do not unpack the firmware image file with the Image command.
3. Select option 1 from the maintenance menu. When prompted for a file name prompt, enter the firmware image file name.

```
Image filename: filename
Unpacking ’filename’, please wait...
Unpackage successful.
```

4. Select option 7 to reset the switch and exit maintenance mode.

5.3.3
Maintenance – Reset Network Config

This option resets the network properties to the factory default values and saves them on the switch. Refer to Table B-6 for the default network configuration values.

5.3.4
Maintenance – Reset Password File

This option restores the password for the Admin account name to the default (password) and removes all other user accounts from the switch.

5.3.5
Maintenance – Copy Log Files

This option copies all log file buffers to a file on the switch named *logfile*. You can use FTP to download this file to the management workstation.

5.3.6
Maintenance – Remove Switch Config

This option deletes all configurations from the switch except for the default configuration. This restores switch configuration parameters to the factory defaults except for user accounts and zoning. Refer to Table B-2 though Table B-6 for the factory default values.

5.3.7
Maintenance – Remake Filesystem

In the event of sudden loss of power, it is possible that the switch configuration may become corrupt. The file system on which the configuration is stored must be re-created. This option resets the switch to the factory default values including user accounts and zoning. Refer to Table B-2 though Table B-6 for the factory default values.

CAUTION! If you choose the **Remake Filesystem** option, you will lose all changes made to the fabric configuration that involve that switch, such as password and zoning changes. You must then reconfigure the portions of the fabric that involve the switch.

5.3.8
Maintenance – Reset Switch

This option closes the Telnet session, exits maintenance mode and reboots the switch using the current switch configuration. All unpacked firmware image files that reside on the switch are deleted.

Section 6
Removal/Replacement

This section describes the removal and replacement procedures for the following field replaceable units (FRU):

- SFP transceivers
- CPU module
- I/O blades
- Cross-connect blades
- Power supply modules
- Fans

Table 6-1 describes the marginal operating configurations based on the number of I/O blades and the number of power supply modules. The marginal operating configurations are intended only to sustain switch operation for the short time until repairs can be made.

Table 6-1. Marginal Operating Configurations

This number of I/O blades . . .	. . .with this number of power supply modules . . .	. . .requires this number of fans.
1–4	1	2
5–8	2	2
5–8	1	3

6.1 SFP Transceivers

The SFP transceivers can be removed and replaced while the switch is operating without damaging the switch or the transceiver. However, transmission on the affected port will be interrupted until the transceiver is installed and reconnected. To remove a transceiver, gently press the transceiver into the port to release the tension, then pull on the release tab or lever and remove the transceiver. Different transceiver manufacturers have different release mechanisms. Consult the documentation for your transceiver.

To install, insert the transceiver into the port and gently press until it snaps in place. The SFP transceiver will fit only one way. If the SFP does not install under gentle pressure, flip it over and try again.

6.2
CPU Module

The CPU module is equipped with a battery that powers the non-volatile memory. This memory stores the switch configuration.

WARNING!! Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of the used battery according to the manufacturer's instructions.

WARNUNG!!

Bei unsachgemäß ausgetauschter Batterie besteht Explosionsgefahr. Die Batterie nur mit der gleichen Batterie oder mit einem äquivalenten, vom Hersteller empfohlenen Batterietyp ersetzen. Die gebrauchte Batterie gemäß den Herstelleranweisungen entsorgen.

AVERTISSEMENT!!

Danger d'explosion si le remplacement de la pile est incorrect. Ne remplacer que par une pile de type identique ou équivalent recommandé par le fabricant. Jeter la pile usagée en observant les instructions du fabricant.

CAUTION! Replacing a CPU module eliminates all switch configuration information. Consult your authorized maintenance provider for assistance in transferring switch configuration data to the new CPU module.

Always use an ESD wrist strap when removing and installing a CPU module. The CPU module contains sensitive logic components. To avoid damage to the module, do not touch the CPU module components. Keep the CPU module in an ESD protective container or anti-static bag when not in use.

6.2.1
Removing the CPU Module

To remove the CPU module, do the following:

1. Determine the firmware version. Open a Telnet session and enter the Show Version command to determine the current firmware version. Make note of the firmware version. If the switch is inaccessible, you can obtain the firmware version from another switch in the fabric or records you may have kept. Refer to "Show Command" on page B-43 for more information.
2. Configure the Telnet window to log output to a file. Enter the Show Support command to document the switch and capture the output on a file.
3. Back up the switch configuration. Enter the Config Backup command to back up the switch configuration to a file on the switch named *configdata*. You can also back up the switch configuration using the Archive function in the SANbox Manager application. Refer to the *SANbox2-64 Switch Management User's Guide* for more information.
4. Back up the event log. Enter the Set Log Archive command to back up the event log to a file on the switch named *logfile*.
5. Download the configuration and log files to your workstation. Open an FTP session to download the *configdata* and *logfile* files onto your workstation. Later, you will restore the switch configuration using the *configdata* file.

```
ftp <ip_address>
User: images
Password: images
ftp> binary
ftp> get configdata
ftp> get logfile
ftp> bye
```

6. Power down the switch. Open a Telnet session and enter the Shutdown command then disconnect the power cords from the power supplies.
7. Label and disconnect the Fibre Channel port cables. This will avoid compromising security and prevent data corruption when the switch is powered up with the new CPU module. Label I/O blades by slot number. I/O blade slots are numbered 1–4 and 6–9. Label Fibre Channel port cables by slot number and port number. Ports on each I/O blade are numbered 0–7 from top to bottom.

8. To unfasten the CPU module, disconnect the Ethernet and serial cables from the CPU module. Connect an ESD wrist strap to a ground point on the chassis or rack. Using a flat-bladed screwdriver, loosen the four captive screws at the top and bottom of the CPU module faceplate as shown in Figure 6-1. The bottom-left screw is under the latch.

CAUTION! The CPU module contains sensitive logic components. To avoid damage to the module, do not touch the CPU module components.

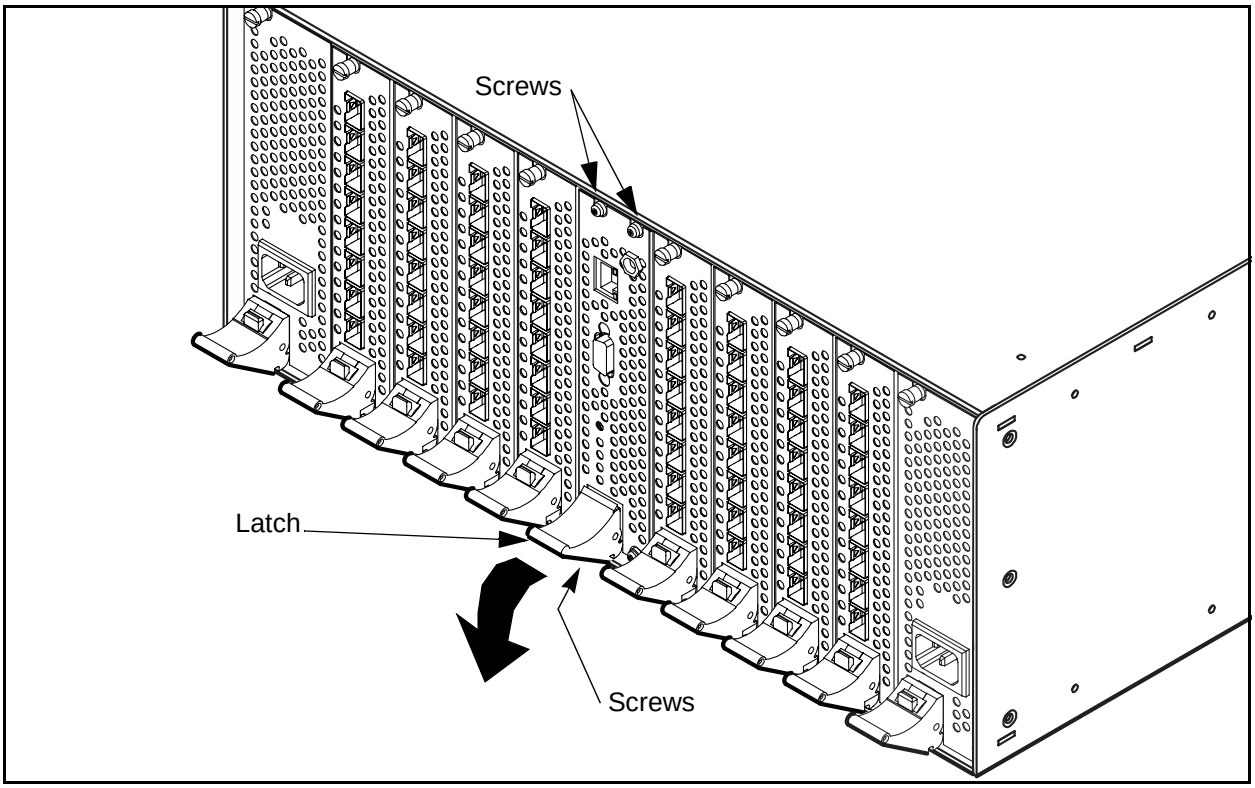


Figure 6-1. Removing the CPU Module

9. To remove the CPU module, grasp the latch and rotate it downward to disengage the CPU module from the backplane connector. Carefully slide the CPU module out of the slot.

6.2.2
Installing the CPU Module

To install the CPU module, do the following:

1. Slide the CPU module into the slot guide until it makes contact with the backplane connector. Rotate the blade latch upward to lock the CPU module in place. Fasten the screws.
2. Reconnect the Ethernet and serial cable to the CPU module.
3. Power up the switch. Reconnect both power cords to the power supply modules.
4. Observe the Heartbeat LED. It should blink once per second. If the Heartbeat LED is showing a different blink pattern, refer to”Heartbeat LED Blink Patterns” on page 5-1 for diagnostic procedures or contact your authorized maintenance provider.
5. Verify the POST results. Open a Telnet session with the default IP address (10.0.0.1), and enter the Show Slot command to display the diagnostic status for the CPU module. Refer to the ”Show Command” on page B-44. You could also display the diagnostic status using the Switch tab or Blade Info tab of the SANbox Manager faceplate display. Refer to the *SANbox2-64 Switch Management User’s Guide*.

   Note: A “Failed” status could indicate a faulty blade or module. Enter the Show POST Log command for more information or contact your authorized maintenance provider.

6. Compare firmware versions. Open a Telnet session and enter the Show Version command to determine the firmware version.
   - If the firmware versions on the two CPU modules are the same, proceed to step 9 to restore the switch configuration.
   - If the firmware versions are different, proceed to step 7 to install firmware.
7. Install firmware. Acquire the firmware image file from your own storage or you can download firmware from the QLogic web site.

8. Load the image file on the switch. Move to the directory that contains the firmware image file and open an FTP session. When prompted, enter the account name (images) and password (images). Enter the Put command and specify the name of the image file.

```
ftp 10.0.0.1
User: images
Password: images
ftp> binary
ftp> put image_file
ftp> bye
```

9. Unpack the image file. Press and hold the Maintenance button for four seconds to place the switch in maintenance mode. Open a Telnet session and log in with the account name “prom” and password “prom”.

```
Telnet 10.0.0.1
Sanbox2 login: prom
Password: prom
```

10. Select option 1 from the maintenance menu. When prompted for a file name enter the firmware image file name. After the unpacking is complete, select option 7 to reset the switch.

```
0) Exit
1) Image Unpack
2) Reset Network Config
3) Reset Password File
4) Copy Log Files
5) Remove Switch Config
6) Remake Filesystem
7) Reset Switch
Option:1

Image filename: image_file
Unpacking 'filename', please wait...
Unpackage successful.


0) Exit
1) Image Unpack
2) Reset Network Config
3) Reset Password File
4) Copy Log Files
5) Remove Switch Config
6) Remake Filesystem
7) Reset Switch
Option:7
```

11. Restore switch configuration. Move to the directory that contains the *configdata* file that you downloaded earlier. Use FTP to upload this file from the management workstation to the switch.

```
ftp 10.0.0.1
User: images
Password: images
ftp> binary
ftp> put configdata
ftp> bye
```

12. Open a Telnet session and enter the Config Restore command to restore the switch configuration. Refer to ”Config Command” on page B-7 for more information. If you archived the configuration using SANbox Manager, you can restore the switch configuration using the SANbox Manager Restore function.
13. Observe the Heartbeat LED. It should blink once per second. If the Heartbeat LED is showing a different blink pattern, refer to ”Heartbeat LED Blink Patterns” on page 5-1 for diagnostic procedures or contact your authorized maintenance provider.
14. Reconnect the Fiber Channel port cables according to their labels. Disconnect the cross-over Ethernet cable and reconnect the original Ethernet cable if there was one.

6.3 I/O Blades

You can remove and install I/O blades while the switch is operating. The following instructions assume that the switch is operating. If you want to maintain service to the devices connected to a particular blade while it is being replaced, transfer the Fibre Channel cables to another blade. To remove an I/O blade blank panel, simply disengage the latch and slide the blank panel from the switch.

CAUTION! The I/O blade contains sensitive logic components. To avoid damage to the I/O blade, do not touch the I/O blade components.

Keep I/O blades in ESD protective containers or anti-static bags when not in use.

To replace an I/O blade, do the following:

1. Label the Fibre Channel port cables by port number. Ports on each I/O blade are numbered 0-7 from top to bottom. Disconnect the Fibre Channel port cables.
2. Put on an ESD wrist strap, and connect it to the ground jack on the CPU module shown in Figure 6-2 or some other ground point on the chassis.

3. Open a Telnet session and enter the Hotswap command. You can also replace an I/O blade using the SANbox Manager application. Perform the tasks as prompted:

Note: The switch will become unresponsive if you do not perform the tasks as prompted. If the switch becomes unresponsive, you must power cycle the switch.

```
SANbox2-64 (admin) #> hotswap

This command will guide you through the hotswap process.
If this process is not followed exactly, then a seamless
transition cannot be guaranteed and a switch power cycle
will be required.
```

4. Choose the Replace task (1).

```
The following procedures may be performed:

1) Replace installed IO blade
2) Insert an IO blade
3) Remove an IO blade
4) Exit this process

Which procedure above do you want to initiate?

(1-4): [4] 1
```

5. Choose the slot number (6 for example).

```
Which IO blade (indexed by slot number) do you want
to replace? (1,2,3,4,6,7,8,9): [1] 6

Are you sure you want to replace the IO blade in slot 6?
(y/n): [n] y
```

6. After confirming that you want to replace the I/O blade, the Port Status LEDs will begin to flash green to positively identify the selected I/O blade. Disconnect all cables from the selected I/O blade.

WARNING!! Voltage is present in an open slot when the switch is operating. To avoid personal injury or damage to components, do not place hands or objects into a slot.

CAUTION! To avoid damaging the latch mechanism, press the red release button all the way in before rotating the latch.

7. Using a flat-bladed screwdriver, loosen the captive screws at the top and bottom of the I/O blade faceplate as shown in Figure 6-2. The bottom screw is under the latch. Grasp the latch and press the red release button, then rotate the latch downward to disengage the I/O blade from the backplane connector. Carefully slide the I/O blade out of the slot.

```
Remove all connections from the IO blade in slot 6.

Remove the IO blade in slot 6 from the chassis.

Please confirm that these steps have been accomplished by
pressing the ENTER key.

Hotswap IO blade removal sub-procedure successfully
completed.
```

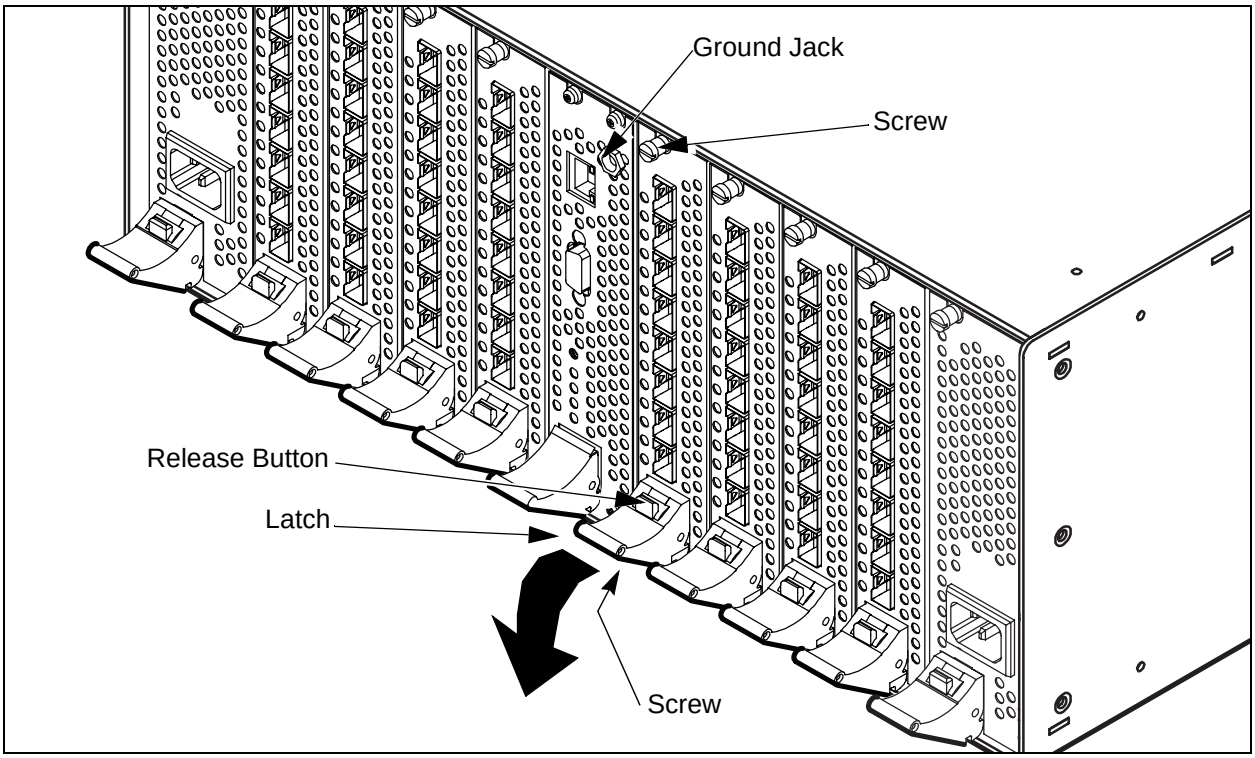


Figure 6-2. Removing an I/O Blade

8. To install a new I/O blade, enter “y”.

```
Do you want to continue with the replacement procedure?
(y/n): [n] y
```

9. Slide the I/O blade into the slot guide until it makes contact with the backplane connector. Rotate the blade latch upward to lock the I/O blade in place. Fasten the screws.

```
Insert the IO blade into the chassis in slot 6.

Attach all connections, if any, to the IO blade in slot 6.

Please confirm that these steps have been accomplished by
pressing the ENTER key.
```

10. After confirming that the I/O blade has been installed, the Port Status LEDs will flash amber in port number sequence, then the Port Status LEDs will flash green. Reconnect the Fiber Channel port cables according to their labels.

11. Verify the POST results. The I/O blade diagnostic status appears in the dialog. The status should be "Passed".

```
Hotswap IO blade process successfully completed.

Diagnostics has been run on the IO blade in slot 7:

Passed
```

Note: A “Failed” status could indicate a faulty blade or module. Enter the Show POST Log command for more information or contact your authorized maintenance provider.

12. The system checks the I/O blades for matching Zircon processor firmware. If any of the I/O blades are not compatible, an alarm message will be generated indicating that a Zircon firmware mismatch has occurred. To display the alarm log, enter the Show Alarm command or use the Alarm Log tab in the SANbox Manager faceplate display. Refer to ”Show Command” on page B-44 for more information. If a mismatch does occur, contact your authorized maintenance provider.

```
SANbox2-64 #> show alarm

[9][Wed Jan 16 13:32:19.500 2003]

[A4101][0xdd0072c2.329][IO-1 Zircon firmware mismatch:
rev 0.5, should be perhaps rev 0.7]
```

6.4

Cross-Connect Blades

The SANbox2-64 switch contains two CC blades: one in slot 11 (CC blade 0) and the other in slot 12 (CC blade 1) as shown in Figure 6-3. You access slot 11 by removing the top-rear switch cover. To access slot 12, you remove the bottom-rear switch cover. Other than this, the procedure for replacing either CC blade is the same.

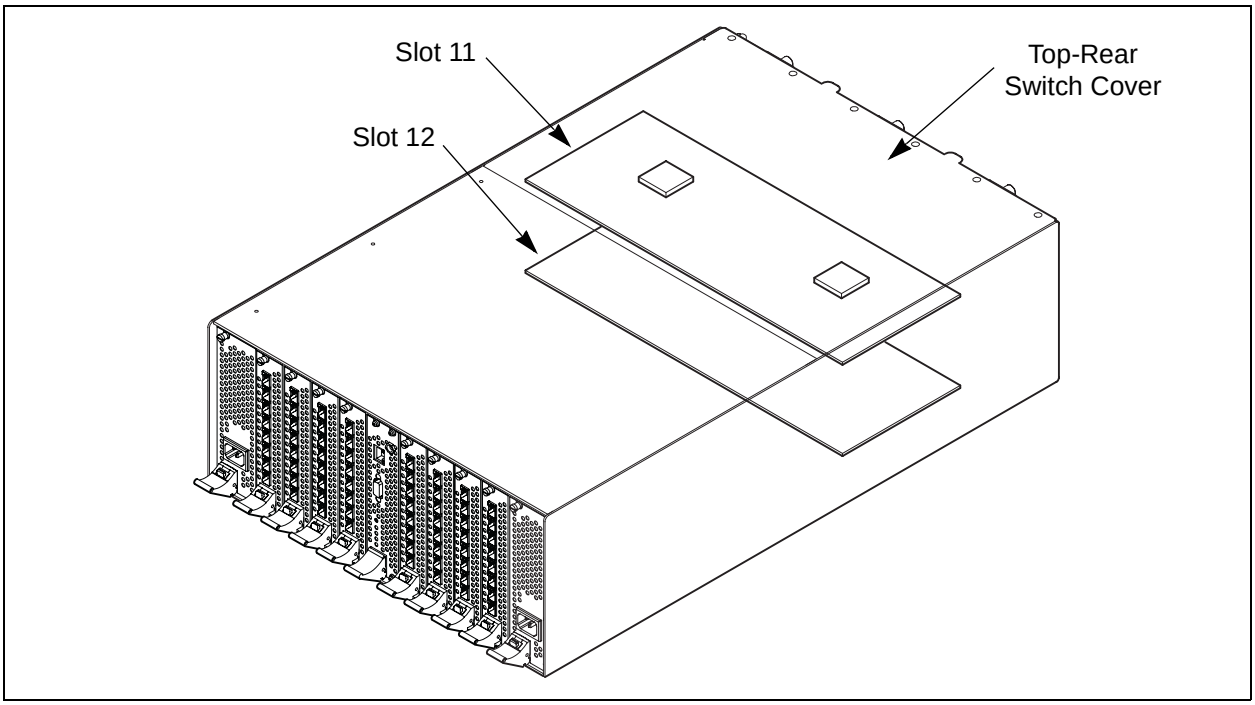


Figure 6-3. CC Blade Slots

CAUTION! Always use an ESD wrist strap when removing and installing a CC blade.

The CC blade contains sensitive logic components. To avoid damage to the module, do not touch the CPU module components.

Keep the CC blade in an ESD protective container or anti-static bag when not in use.

6.4.1
Removing a CC Blade

To remove a CC blade, do the following:

1. Power down the switch. Isolate the switch from the fabric. Open a Telnet session and enter the Shutdown command. Disconnect the power cords from the power supplies.

```
telnet <ip_address>

SANbox2 Login: admin
Password: password

Sanbox2-64 #> admin start
Sanbox2-64 (admin) #> shutdown

The switch will shutdown. Please confirm (y/n): [n] y
Shutdown in progress...

Please wait at least 20 seconds before powering off
the switch or loss of data may result.
```

2. Label the Fibre Channel port cables by slot number and port number. I/O blade slots are numbered 1–4 and 6–9. Ports on each I/O blade are numbered 0–7 from top to bottom.
3. Put on an ESD wrist strap. Connect it to the ground jack on the CPU module or to another chassis ground point. Disconnect Fibre Channel port cables.
4. Disconnect Ethernet and serial cables.

WARNING!! Two people are required to safely lift and install the switch into a cabinet. To avoid personal injury or damage to the switch, arrange for assistance

5. Remove the switch from the rack. Using a crosshead screw driver, remove the screws that secure the switch brackets to the rack. Slide the switch out of the rack until the rail latches drop down to stop the switch. Lift up on the latches on both sides and finish removing the switch.

6. Remove the switch cover. Use a medium crosshead screw driver to remove the four screws on each side and the six screws on top as shown in Figure 6-4. Lift and remove the switch cover and set it aside. Put on an ESD wrist strap and connect it to ground.

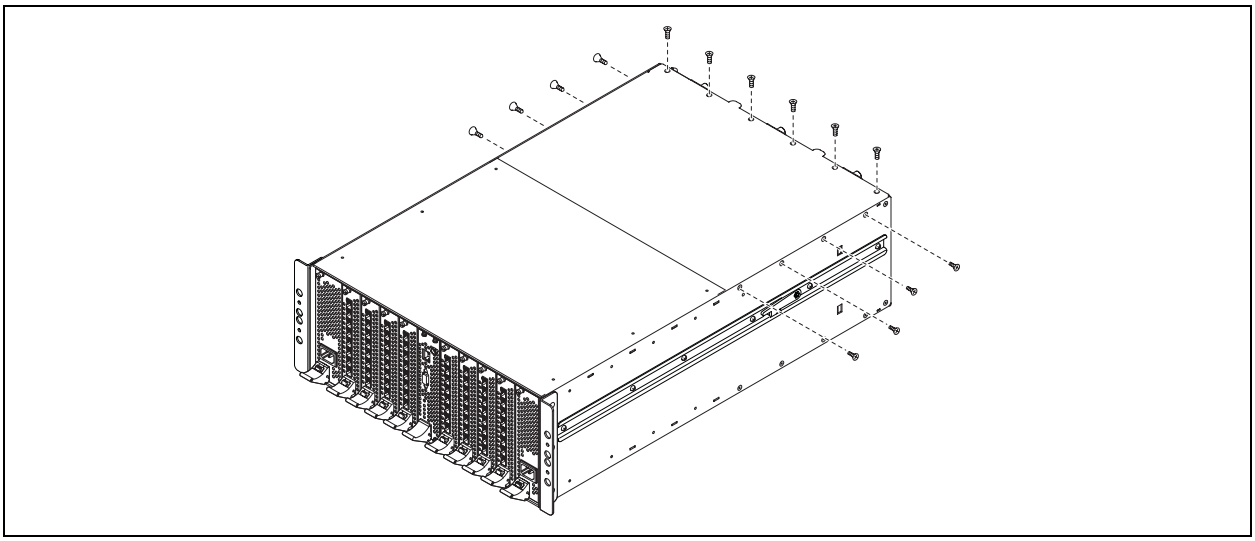


Figure 6-4. Switch Cover Removal

7. Remove the CC blade. Loosen the six screws (1) that fasten the CC blade to the chassis as shown in Figure 6-5, but do not remove them. The three screws nearest the latches (2) need only be loosened a couple turns. The three screws nearest the backplane (3) must be backed off about 3/8 of inch to allow enough clearance to remove the blade.

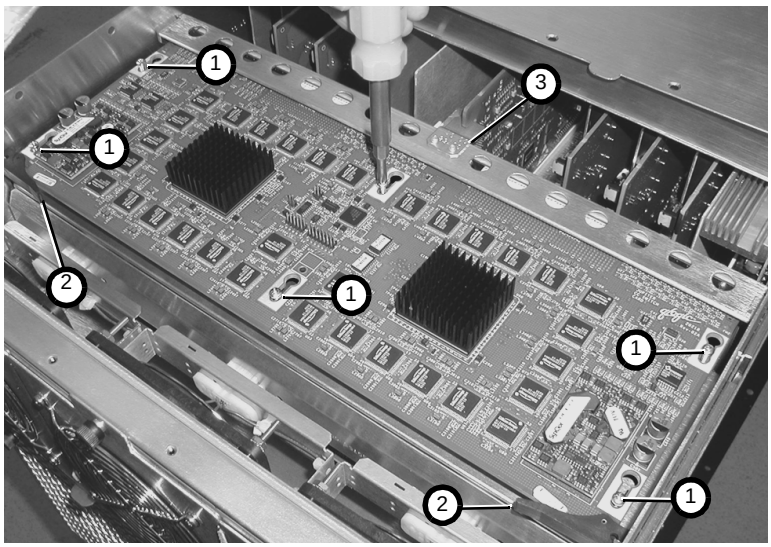


Figure 6-5. CC Blade Removal

8. Disconnect the CC blade from backplane. Grasp both latches with the thumbs. Open both latches together a little at a time to disengage the CC blade from the backplane.
9. Lift CC blade from switch. Using the thumbs under the open latches, lift the latch edge of the CC blade up enough to get a better grip. Gently lift the CC blade from the switch. If the CC blade will not come off the screws nearest the backplane, back the screws off a little more. Place the CC blade in an anti-static bag.

6.4.2 Installing a CC Blade

To install a CC blade, do the following:

1. Put on an ESD wrist strap. Connect it to the ground jack on the CPU module or to another chassis ground point.
2. Remove the new CC blade from its packaging. Open both latches all the way. Holding the CC blade by the latches, place the blade in the switch. Center the blade key holes over the screws nearest the backplane, then lower the blade over the remaining screws as shown in Figure 6-6.

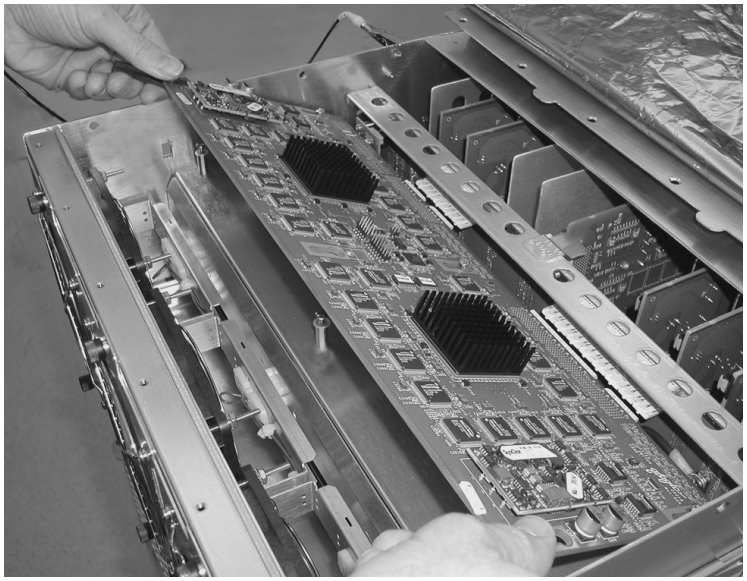


Figure 6-6. Installing a CC Blade

3. Using the thumbs, close both latches to seat the CC blade in the backplane. When securing the latches, be sure that the latch engages the chassis tab. Using a crosshead screw driver, fasten the blade screws finger tight beginning with the two middle screws.
4. Replace the switch cover and fasten all the screws.

WARNING!! Two people are required to safely lift and install the switch into a cabinet. To avoid personal injury or damage to the switch, arrange for assistance

5. With an assistant, slide the switch into the rack. Fasten the switch brackets to the rack with screws.
6. Reconnect the Ethernet cable to the CPU module. Reconnect the power cords to the power supply modules to power up the switch.
7. Confirm the power supply module status. Do one of the following:
   - Open a Telnet session and enter the Show Slot command to display the operational status of the CC blades. Refer to the "Show Command" on page B-44.
   - Observe the CC blade status in the Switch or the Blade Info data windows of the SANbox Manager faceplate display. Refer to the *SANbox2-64 Switch Management User's Guide*.

Note: A "Failed" status could indicate an improperly seated or faulty blade. Enter the Show POST Log command for more information or contact your authorized maintenance provider.

6.5 Power Supply Modules

The power supply modules are hot pluggable. This means you can remove or install one of the two functioning power supply modules without disrupting service. The power supply modules are also interchangeable; that is, any power supply module will fit in slot #0 or slot #10.

6.5.1 Removing a Power Supply Module

To remove a power supply module, do the following:

WARNING!! The power supply module faceplate and internal surfaces can become very hot. Handle with care.

Voltage is present in an open slot when the switch is operating. To avoid personal injury or damage to surrounding components, do not place hands or objects into an open slot.

CAUTION! Always use an ESD wrist strap when removing and installing a power supply module. The power supply module contains sensitive electronic components. To avoid damage to the power supply module, do not touch the module components.

Keep the power supply module in an ESD protective container or anti-static bag when not in use.

1. Disconnect the power cord from the power supply module.
2. Connect an ESD wrist strap to the ground jack on the CPU module shown in Figure 6-7 or some other ground point on the chassis.
3. Using a flat-blade screw driver, loosen the captive screws at the top and bottom of the module faceplate as shown in Figure 6-7. The bottom screw is under the latch.

CAUTION! To avoid damaging the latch mechanism, press the red release button all the way in before rotating the latch.

4. Grasp the latch and press the red release button, then rotate the latch downward to disengage the module from the backplane connector. Carefully slide the module out of the slot.

CAUTION! To prevent overheating and possible damage to the switch, do not operate the switch with an empty slot any longer than it takes to install a new power supply module.

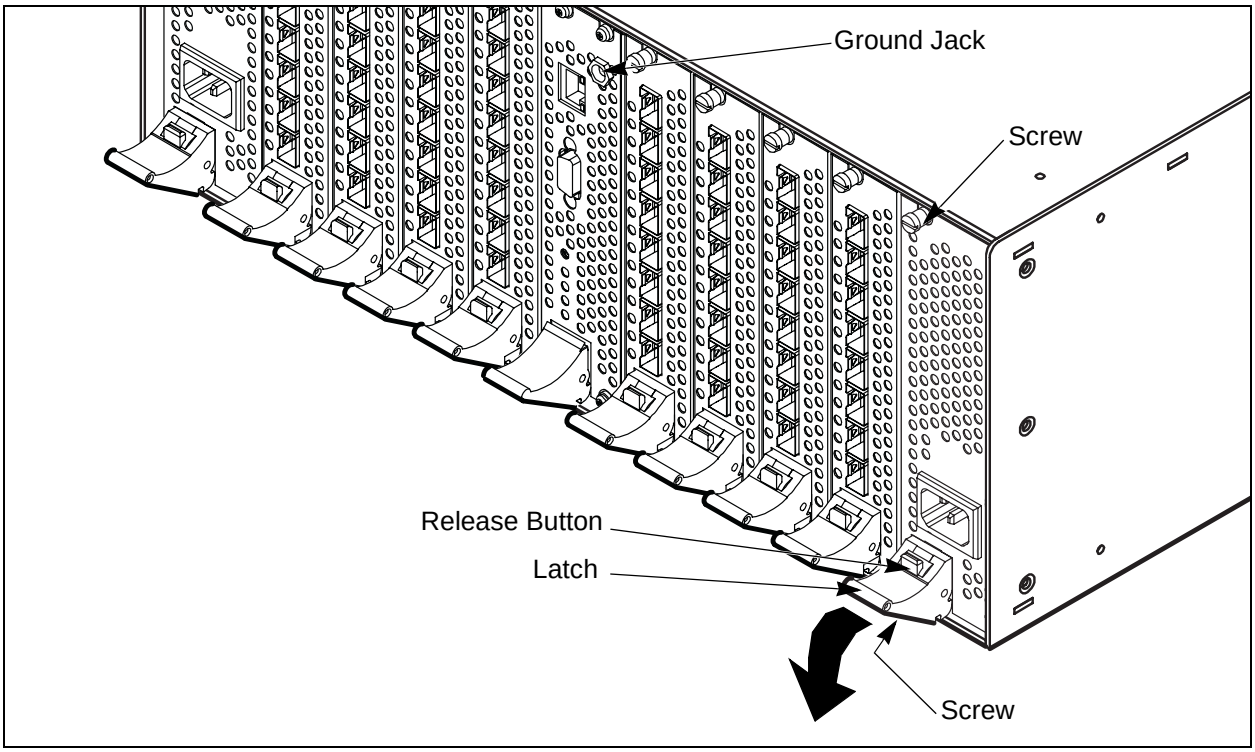


Figure 6-7. Removing a Power Supply Module

6.5.2

Installing a Power Supply Module

To install a power supply module, do the following:

1. Slide the power supply module into the slot guide until it contacts the backplane.
2. Rotate the blade latch upward to lock the power supply module in place. Fasten the screws.
3. Reconnect the power cord to the power supply module and confirm that the Output Power LED illuminates.
4. Confirm the power supply module status. Do one of the following:
   - Open a Telnet session and enter the Show Chassis command to display the operational status of the power supply modules. Refer to the ”Show Command” on page B-44.
   - Observe the power supply status in the Switch data window of the SANbox Manager topology display. Refer to the *SANbox2-64 Switch Management User’s Guide*.

6.6 Fans

The fans are hot pluggable. This means you can remove or install one of the fans while the switch is operating without disrupting service. The fan is completely enclosed, so there is no risk of injury from the fan blades. The fans are also interchangeable; that is, any fan will fit in any bay. Before removing a fan, connect an ESD wrist strap to a ground point on the chassis or rack.

6.6.1 Removing a Fan

To remove a fan, loosen the two captive screws shown in Figure 6-8 with a flat-blade screw driver. Grasp the fan by the screws and pull firmly to disengage the fan from the backplane connector. Slide the fan out of the chassis.

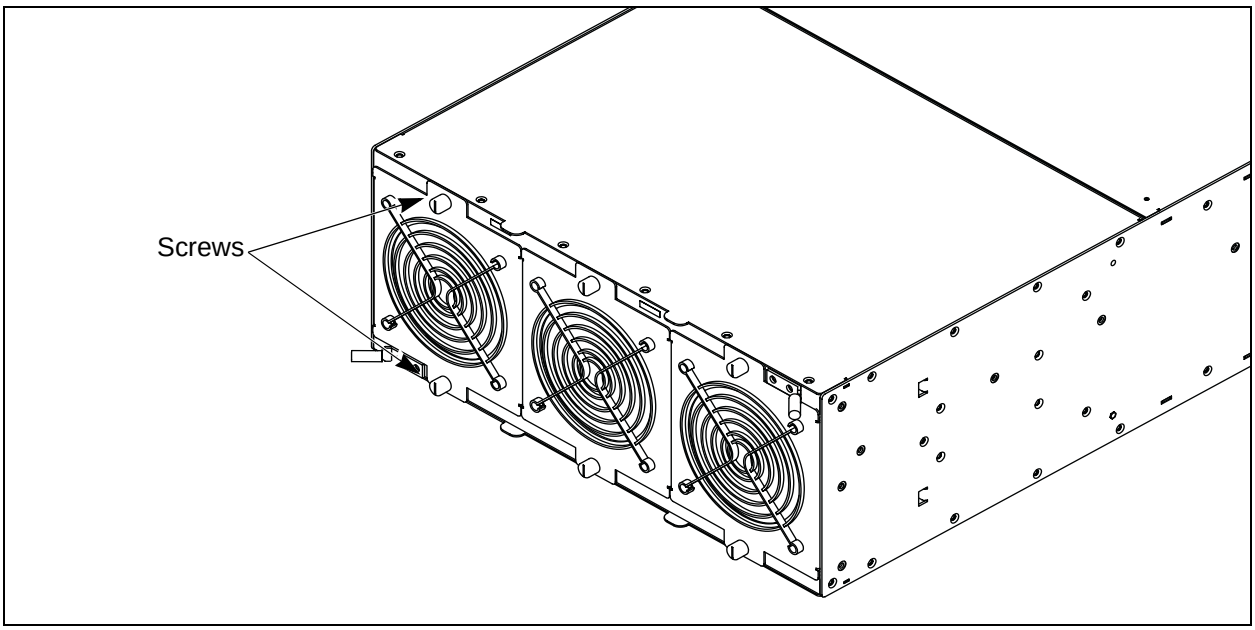


Figure 6-8. Removing a Fan

WARNING!! Voltage is present in an open bay when the switch is operating. To avoid personal injury, do not place hands or objects into an open bay.

CAUTION! Replacement fans must be compatible with the switch air flow direction of the other fans. Installing a fan with an opposing air flow direction could lead to an over temperature condition.

To avoid overheating, do not operate the switch without a fan any longer than it takes to install a new fan.

6.6.2
Installing a Fan

To install a fan, do the following:

1. Confirm that the new fan has the same air flow direction as the old fan. Each fan has a label indicating the air flow direction.
2. Slide the fan into the bay until it is firmly seated and fasten the screws. A fan will fit in any bay.
3. Confirm the fan status. Do one of the following:
   - Open a Telnet session and enter the Show Chassis command to display the operational status of the fans. Refer to the ”Show Command” on page B-44.
   - Observe the fan status in the Switch data window of the SANbox Manager topology display. Refer to the *SANbox2-64 Switch Management User’s Guide*.

Notes

Appendix A
Specifications

Appendix A contains the specifications for the SANbox2-64 Fibre Channel switch. Refer to Section 2 General Description for the location of all controls and components.

A.1 Performance

Fibre Channel Protocols	FC-PH Rev. 4.3 FC-PH-2 FC-PH-3 FC-AL Rev 4.5 FC-AL-2 Rev 7.0 FC-FLA FC-GS-3 FC-FG FC-PLDA FC-Tape FC-VI FC-SW-2 Fibre Channel Element MIB RFC 2837 Fibre Alliance MIB Version 4.0
Fibre Channel Classes of Service ..	Classes 2 and 3 connectionless
Port Types.....	F_Port FL_Port TL_Port E_Port G_Port GL_Port
Port Characteristics	All ports are auto-discovering and self-configuring.
Number of Fibre Channel Ports	8 ports per I/O blade; maximum of 64 total ports
Scalability.....	Maximum 239 switches depending on configuration
Maximum User Ports	> 475,000 ports depending on configuration

Buffer Credits	12 buffer credits per port
Media Type	Small Form Pluggable (SFP) optical transceivers. Hot pluggable. 3.3 Volts.
Fabric Port Speed	1.0625 or 2.125 Gigabits/second
Maximum Frame Size	2148 bytes (2112 byte payload)
System Processor	850 MHz Pentium III® processor
Fabric Latency (best case)	<0.5 µsec.
Fabric Point-to-Point Bandwidth	212 or 424 MB/s full duplex
Fabric Aggregate Bandwidth	Scalable from 64 Gb/s end-to-end to 256 Gb/s full bandwidth cross-bar; non-blocking architecture

A.2 Maintainability

Maintenance Strategy	Field Replaceable Units ■ SFP transceivers ■ CPU module ■ I/O blades (8 maximum) ■ Power supply modules (2) ■ Fans (3)
Diagnostics	Power On Self Test (POST) tests all functional components except SFP transceivers.
User Interface	LED indicators on I/O blades, CPU module, and power supply modules

A.3 Fabric Management

Management Methods	SANbox Manager Graphical User Interface Application Programming Interface Command Line Interface GS-3 Management Server SNMP FTP
Maintenance Connection	RS-232 connector; null modem F/F DB9 cable
Ethernet Connection	RJ-45 connector; 10/100BASE T cable
Switch Agent	Allows a network management station to obtain configuration values, traffic information, and failure data pertaining to the Fibre Channels through SNMP through the Ethernet interface.

A.4 Dimensions

Width	17.0” (431 mm), 19 inch rack mount
Height	7.0” (179 mm) (4U)
Depth	27.75.” (705 mm)
Weight	70 lbs (31.75 Kg)

A.5 Electrical

Power source loading	11.5 Amps maximum at 90 to 137 VAC 7.5 Amps maximum at 138 to 264 VAC
Heat Output (maximum)	1000 Watts fully populated (8 I/O blades at ~60 Watts each)
Operating voltage	90 to 264 Vac; 47 to 63 Hz
Circuit Protection	Internally fused

A.6 Environmental

Temperature	
■ Operating	5 to 40°C (41 to 122°F)
■ Non-operating	- 40 to 70°C (-40 to 158°F)
Humidity	
■ Operating	15% to 80%, non-condensing
■ Non-operating	5% to 90%, non-condensing
Altitude	
■ Operating	0 to 3048m (0 to 10,000 feet)
■ Non-operating	0 to 15,240m (0 to 50,000 feet)
Vibration	Magnitude during/after along any axis
■ Operating	5-500 Hz, random, 0.21 G rms, 10 minutes
■ Non-operating	5-500 Hz, random, 2.09 G rms, 10 minutes
Shock	Magnitude during/after along any axis
■ Operating	4 g, 11ms, 20 repetitions
■ Non-operating	30g, 292 ips, 3 repetitions, 3 axis
Air flow	Three fans; front-to-back or back-to-front air flow depending on the model

A.7 Regulatory Certifications

Safety Standards	UL60950, CSA 22.2 No. 950, EN60950
Emissions Standards	FCC Part 15B Class A VCCI Class A ITE BSMI Class A CISPR 22, Class A EN 55022, Class A
Voltage Fluctuations	EN 61000-3-3
Harmonics	EN 61000-3-2
Immunity	EN 55024:1998
Marking	FCC Part 15,UL (United States), cUL (Canada), TUV, VCCI, BSMI, CE

A.8 Shortwave Laser SFP 1G/2G (multi-mode)

Connector	Duplex LC
Color coding	Beige or black exposed connector surfaces
Cable	Fibre Channel 100-M6-SN-I (50 µm multimode) Fibre Channel 200-M5-SN-I or 200-M6-SN-I (62.5 µm multimode)
Wavelength	830 - 860 nm
Transmit Power	-10 dBm minimum
Receiver Sensitivity	-16 dBm average
Distance	500 meters maximum using 50 micron fiber 300 meters maximum using 62.5 micron fiber
Safety	DHHS 21 CFR(J), IEC 825-1 CENELEC EN 60825-1, VDE
Standard	Small Form-Factor Pluggable Multisource Agreement

A.9
Longwave Laser SFP 1G/2G (single-mode)

Connector	Duplex LC
Color coding	Blue exposed connector surfaces
Cable	Fibre Channel 100SM-LC-L (9 µm single mode)
Wavelength	1270 - 13.5 nm
Transmit Power	-10 dBm minimum
Receiver Sensitivity	-20 dBm average
Distance	2 meters to 10 kilometers
Safety	DHHS 21 CFR(J), IEC 825-1 CENELEC EN 60825-1, VDE
Standard	Small Form-Factor Pluggable Multisource Agreement

Appendix B
Command Line Interface

Each switch contains a Telnet server. This server allows a Telnet client to establish a Telnet session with the switch to retrieve information or to configure parameters using the Command Line Interface (CLI). The CLI enables you to perform a variety of fabric and switch management tasks through an Ethernet or a serial port connection.

B.1 Logging On to a Switch

To log on to a switch using Telnet, open a command line window on the management workstation and enter the Telnet command followed by the switch IP address:

```
/> telnet 123.45.67.89
```

A Telnet window opens prompting you for a login. Enter an account name and password. Switches come from the factory with the following user account already defined:

Account name: admin
Password: password
Authority: Admin

This user account provides full access to the switch and its configuration. After planning your fabric management needs and creating your own user accounts, consider changing the password for this account. Refer to ”Commands” on page B-3 for more information about authority levels. Refer to the ”User Command” on page B-70 for information about creating user accounts.

Note: A switch supports a combined maximum of 15 logins. This includes SANbox Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins and Telnet logins. Of this 15, there can be a combined maximum of 10 SANbox Manager and API logins. Additional logins will be refused.

B.2 Command Syntax

The command syntax is as follows:

command
keyword
keyword *[value]*
keyword [value1] [value2]

The **Command** is followed by one or more keywords. Consider the following rules and conventions:

- Commands and keywords are lowercase and case sensitive.
- Commands with keywords require one of those keywords.
- Required keyword values appear in standard font: [value]. Optional values are shown in italics: *[value].*
- Underlined portions of the keyword in the command format indicate the abbreviated form that can be used. For example the Delete keyword can be abbreviated Del.

B.3 Commands

The command set provides for User and Admin authority levels.

- User authority grants viewing access to the fabric and switches using the Show command and other read-only commands.
- Admin authority includes the User authority and grants permission to use the Admin command. The Admin Start command opens an admin session which provides access to the commands that change switch and fabric configurations. Refer to the "Admin Command" on page B-4.

Note: Admin authority is enforced only if fabric security is enabled. By default, fabric security is disabled. Refer to "Set Setup Command" on page B-40 (System keyword) for more about setting fabric security.

The commands and their page numbers are listed by authority level in Table B-1.

Table B-1. Commands Listed by Authority Level

User Authority Commands		Admin Authority Command	
Help	(B-11)	Admin	(B-4)
History	(B-12)	**Admin Session Commands**	
Ps	(B-18)		
Quit	(B-19)	Alias[1]	(B-5)
Show	(B-44)	Config[1]	(B-7)
Show Config	(B-55)	Date[1]	(B-9)
Show Log	(B-58)	Fallback	(B-10)
Show Perf	(B-60)	Hotswap	(B-13)
Show Setup	(B-62)	Image	(B-15)
Uptime	(B-69)	Lip	(B-16)
Whoami	(B-72)	Passwd	(B-17)
		Reset	(B-20)
		Set[1]	(B-25)
		Set Config	(B-27)
		Set Log	(B-35)
		Set Port	(B-38)
		Set Setup	(B-40)
		Shutdown	(B-65)
		Test	(B-66)
		User[1]	(B-70)
		Zone[1]	(B-73)
		Zoneset[1]	(B-77)
		Zoning[1]	(B-79)

[1]Some keywords are available with User authority.

Admin Command

Opens and closes an Admin session. The Admin session provides commands that change the fabric and switch configurations. Only one Admin session can be open on the switch at any time. An inactive Admin session will time out after a period of time which can be changed using the Set Setup System command. Refer to the "Set Setup Command" on page B-40.

Authority Admin

Syntax

admin
start
end
cancel

Keywords

start
Opens the admin session.

end
Closes the admin session. The Logout, Shutdown, and Reset Switch commands will also end an admin session.

cancel
Terminates an Admin session opened by another user. Use this keyword with care because it terminates the Admin session without warning the other user and without saving pending changes.

Notes Closing a Telnet window during an admin session does not release the session. In this case, you must either wait for the admin session to time out, or use the Admin Cancel command.

Examples The following example shows how to open and close an Admin session:

```
SANbox2-64 N108 #> admin start

SANbox2-64 N108 (admin) #>

.
.
.

SANbox2-64 N108 (admin) #> admin end
```

Alias Command

Creates a named set of ports/devices. Aliases make it easier to assign a set of ports/devices to many zones. An alias can not have a zone or another alias as a member.

Authority Admin

Syntax **alias**

add [alias] [members]
copy [alias_source] [alias_destination]
create [alias]
delete [alias]
list
members [alias]
remove [alias] [members]
rename [alias_old] [alias_new]

Keywords

add [alias] [members]
Specifies one or more ports/devices given by [members] to add to the alias named [alias]. An alias can have a maximum of 2000 members. [members] can have one of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs and port numbers are in decimal. Ports are numbered beginning with 0.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.

The application verifies that the [alias] format is correct, but does not validate that such a port/device exists.

copy [alias_source] [alias_destination]
Creates a new alias named [alias_destination] and copies the membership into it from the alias given by [alias_source].

create [alias]
Creates an alias with the name given by [alias]. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, and -. The zoning database supports a maximum of 256 aliases.

delete [alias]
Deletes the specified alias given by [alias] from the zoning database. If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all aliases. This keyword is valid for User authority and does not require a zoning edit session or an admin session.

members [alias]
Displays all members of the alias given by [alias]. This keyword is available with User authority and does not require a zoning edit session or an admin session.

remove [alias] [members]
Removes the ports/devices given by [members] from the alias given by [alias]. [members] can have one of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs and port numbers are in decimal. Ports are numbered beginning with 0.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) for the device with the format xx:xx:xx:xx:xx:xx:xx:xx.

rename [alias_old] [alias_new]
Renames the alias given by [alias_old] to the alias given by [alias_new].

Config Command

Manages the Fibre Channel configurations on a switch. For information about setting the port and switch configurations, refer to the "Set Config Command" on page B-27.

Authority Admin for all keywords except List

Syntax

config
activate *[config]*
backup
cancel
copy [config_source] [config_destination]
delete [config]
edit *[config]*
list
restore
save *[config]*

Keywords

activate *[config]*
Activates the configuration given by [config]. If you omit the configuration, the currently active configuration is used. Only one configuration can be active at a time.

backup
Creates a file named *configdata*, which contains the system configuration information. To download this file, open an FTP session, log in with account name/password of "images" for both, and type "get configdata".

cancel
Terminates the current configuration edit session without saving changes that were made.

copy [config_source] [config_destination]
Copies the configuration given by [config_source] to the configuration given by [config_destination]. The switch supports up to 10 configurations including the default configuration.

delete [config]
Deletes the specified configuration file where [config] is a file name.

edit *[config]*
Opens an edit session for the configuration given by [config]. If you omit the configuration name, the currently active configuration is used.

list
Displays a list of all available configurations. This keyword is available with User authority.

restore
Restores configuration settings to an out-of-band switch from a backup file named *configdata*, which must be first uploaded on the switch using FTP. You create the backup file using the Config Backup command. Use FTP to load the backup file on a switch, then enter the Config Restore command.

Note: Configuration archive files created with the SANbox Manager Archive function are not compatible with the Config Restore command.

save *[config]*
Saves changes made during a configuration edit session in the configuration given by [config]. If you omit the configuration name value, the configuration you chose for the Config Edit command is used. The switch supports up to 10 configurations including the default configuration.

Notes

If you edit the active configuration, changes will be held in suspense until you reactivate the configuration or activate another configuration.

Examples

The following shows an example of how to open and close a Config Edit session:

```
SANbox2-64 N108 #> admin start

SANbox2-64 N108 (admin) #> config edit
.
.
.
SANbox2-64 N108 (admin-config) #>> config cancel

  Configuration mode will be canceled.Please confirm (y/n): [n] y

SANbox2-64 N108 (admin) #> admin end
```

Date Command

This command displays or sets the system date and time. To set the date and time the information string must be provided in this format: MMDDhhmmCCYY. You must reset the switch for the new date to take effect.

Authority Admin to change the date; User to display the date.

Syntax **date**
[MMDDhhmmCCYY]

Keywords ***[MMDDhhmmCCYY]***
Specifies the date – this requires an admin session. If you omit [MMDDhhmmCCYY], the current date is displayed – this is available with User authority.

Examples The following is an example of the Date command:

```
SANbox2-64 N108 #> date
  Tue Nov 12 07:51:24 2002
```

Fallback Command

Loads the fallback version of the firmware from switch memory. The switch stores two versions of the firmware. This command alternately activates the two versions.

Authority Admin

Syntax **fallback**

Notes

- The Show Switch command displays the available firmware versions and the currently active version.
- After executing the Fallback command, reset the switch for the firmware to be placed in effect.

Examples The following is an example of the Fallback command:

```
SANbox2-64 N108 #> admin start

SANbox2-64 N108 (admin) #> fallback

  Reverting to previous software image.  Please confirm (y/n): [n] y

SANbox2-64 N108 #> admin end
```

Help Command

Displays a brief description of the specified command and its keywords.

Authority User

Syntax **help *[command] [keyword]***

Keywords ***[command]***
Displays a summary of the command given by [command] and its keywords. If you omit [command], the system displays all available commands from which to choose.

[keyword]
Displays a summary of the keyword given by [keyword] belonging to the command given by [command]. If you omit [keyword], the system displays the available keywords for the specified command.

all
Displays a list of all available commands (including command variations).

Examples The following is an example of the Help Set command:

```
SANbox2-64 N108 #> help set

set SET_OPTIONS
There are many attributes that can be set.
Type help with one of the following to get more information:
    set alarm
    set beacon
    set blade
    set config blade
    set config port
    set config ports
    set config switch
    set config threshold
    set config zoning
    set log
    set pagebreak
    set port
    set setup snmp
    set setup system
    set switch
```

The following is an example of the Help Set Beacon command:

```
SANbox2-64 N108 #> help set beacon
set beacon On | Off
This command allows the LEDs on the front of the switch to flash.
The On option will start and the Off option will stop the flashing.
```

History Command

Displays a numbered list of the previously entered commands from which you can re-execute selected commands.

Authority User

Syntax **history**

Notes Use the History command to provide context for the ! command:

- Enter ![command] to re-enter the most recent execution of that command.
- Enter ![line number] to re-execute the corresponding command from the History display
- Enter ![partial command string] to re-execute a command that matches the command string.
- Enter !! to re-execute the most recent command.

Examples The following is an example of the History command:

```
SANbox2-64 N108 #> history
   1 show switch
   2 date
   3 help set
   4 history

SANbox2-64 N108 #> !3
help set

set SET_OPTIONS
There are many attributes that can be set.
Type help with one of the following to get more information:
    set alarm
    set beacon
    set blade
    set config blade
    set config port
    set config ports
    set config switch
    set config threshold
    set config zoning
    set log
    set pagebreak
    set port
    set setup snmp
    set setup system
    set switch
```

Hotswap Command

This command prompts you step-by-step through the procedure to replace an I/O blade, insert an I/O blade, or remove an I/O blade while the switch is running.

Authority Admin

Syntax **hotswap**

Notes The Hotswap command automatically starts and ends an Admin session in the presence of admin authority.

Always perform the hot swap procedure as prompted, otherwise the switch will become unresponsive. For example, if you install a blade in the wrong slot, proceed as though you no mistake had been made and follow the rest of the procedures. When complete, perform the operation again with the correct slot. If the switch becomes unresponsive, you must power cycle the switch.

After you select an I/O blade to remove and press the Enter key, all Port Status LEDs will flash green to identify the selected I/O blade.

After you install an I/O blade and press the Enter key, the Port Status LEDs will flash amber in sequence by port number, then the Port Status LEDs will flash green.

Examples The following is an example of the Hotswap Replace command:

```
SANbox2-64> hotswap
This command will guide you through the hotswap process. If this process is not
followed exactly, then a seamless transition cannot be guaranteed and a switch
power cycle will be required.
The following procedures may be performed:
1) Replace installed IO blade
2) Insert an IO blade
3) Remove an IO blade
4) Exit this process
Which procedure above do you want to initiate?
(1-4): [4] 1

Which IO blade (indexed by slot number) do you want
to replace? (1,2,3,4,6,7,8,9): [1] 6
Are you sure you want to replace the IO blade in slot 6? (y/n): [n] y
Remove all connections from the IO blade in slot 6.
Remove the IO blade in slot 6 from the chassis.
Please confirm that these steps have been accomplished by pressing the ENTER key.
Hotswap IO blade removal sub-procedure successfully
completed.

Do you want to continue with the replacement procedure? (y/n): [n] y
Insert the IO blade into the chassis in slot 6.
```

```
Attach all connections, if any, to the IO blade in slot 6.
Please confirm that these steps have been accomplished by pressing the ENTER key.
Hotswap IO blade process successfully completed.
Diagnostics has been run on the IO blade in slot 6:
Passed
```

Image Command

Manages and installs switch firmware.

Authority Admin

Syntax

image
cleanup
fetch [account_name] [ip_address] [file_source] [file_destination]
list
unpack [file]

Keywords

cleanup
Removes all firmware image files from the switch. All firmware image files are removed automatically each time the switch is reset.

fetch [account_name] [ip_address] [file_source] [file_destination]
Retrieves image file given by [file_source] and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the device with the IP address given by [ip_address] and an account name given by [account_name]. If an account name needs a password to access the device, the system will prompt you for it.

list
Displays the list of image files that reside on the switch.

unpack [file]
Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch must be reset for the new firmware to take effect.

Notes To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

Lip Command

Reinitializes the specified loop port.

Authority Admin

Syntax **lip [port_number]**

Keywords **[port_number]**
The number of the port to be reinitialized.

Examples The following is an example of the Lip command:

```
SANbox2-64 N108 (admin) #> lip 2
```

Passwd Command

Changes a user account's password.

Authority Admin to change another account's password; User to change your own.

Syntax **passwd [account_name]**

Keywords **[account_name]**
The user account name. You must open an admin session to change the password for an account name other than your own. If you omit [account_name], you will be prompted to change the password for the current account name.

Examples The following is an example of the Passwd command:

```
SANbox2-64 N108 (admin) #> passwd user2

     Press 'q' and the ENTER key to abort this command.

  account OLD password               :
  account NEW password (4-20 chars)  :

  please confirm account NEW password:

  password has been changed.
```

Ps Command

Displays current system process information.

Authority User

Syntax **ps**

Examples The following is an example of the Ps command:

```
SANbox2-64 N108 #> ps
 PID  PPID %CPU     TIME     ELAPSED COMMAND
  298   287  0.0 00:00:00  4-01:33:01 cns
  299   287  0.0 00:00:00  4-01:33:01 ens
  300   287  0.0 00:00:00  4-01:33:01 dlog
  301   287  0.0 00:00:41  4-01:33:01 ds
  302   287  0.9 00:57:58  4-01:33:01 mgmtApp
  325   287  0.0 00:00:00  4-01:32:29 fc2
  326   287  0.0 00:00:00  4-01:32:29 nserver
  327   287  0.0 00:00:00  4-01:32:29 mserver
  328   287  0.0 00:00:07  4-01:32:29 util
  330   287  0.0 00:00:02  4-01:32:29 snmpservicepath
  331   287  0.0 00:00:00  4-01:32:29 eport
  332   287  0.0 00:05:10  4-01:32:29 PortApp
  334   287  0.0 00:00:00  4-01:32:29 port_mon
  335   287  0.0 00:00:00  4-01:32:29 zoning
  336   287  0.0 00:00:00  4-01:32:29 diagApp
  414   287  0.0 00:00:00  4-01:31:51 snmpd
  415   287  0.0 00:00:00  4-01:31:51 snmpmain
  416   415  0.0 00:00:00  4-01:31:51 snmpmain
  417   416  0.0 00:00:00  4-01:31:51 snmpmain
```

Quit Command

Closes the Telnet session.

Authority User

Syntax **quit, exit, or logout**

Reset Command

Resets the switch and port configuration parameters.

Authority Admin

Syntax **reset**

blade [slot_number]
config *[config_name]*
factory
port [port_number]
snmp
switch (default)
system
zoning

Keywords

blade [slot_number]
Resets the I/O or cross-connect blade that occupies the slot given by [slot_number]. I/O blade slot numbers are 1–4 and 6–9; cross-connect slot numbers are 11–12.

config *[config_name]*
Resets the configuration given by [config_name] to the factory default values for switch, port, alarm threshold, and zoning configuration. This keyword clears all zoning definitions. If [config_name] does not exist on the switch, a configuration with that name will be created. If you omit [config_name], the active configuration is reset. You must activate the configuration or reset the switch for the changes to take effect. Refer to Table B-2 through Table B-4 for switch, port, and alarm threshold configuration default values.

factory
Resets switch, alarm threshold, zoning, SNMP, zoning configuration, and system configuration settings to the factory default values. The switch configuration is activated automatically. Refer to Table B-2 through Table B-6.

port [port_number]
Reinitializes the port given by [port_number]. Ports are numbered beginning with 0.

snmp
Resets the SNMP configuration settings to the factory default values. Refer to Table B-5 for SNMP configuration default values.

switch
Reinitializes the switch. This is the default. This command also closes the Telnet session.

system
Resets the system configuration settings to the factory default values. Refer to Table B-6 for system configuration default values.

zoning
Clears the zoning database and deactivates the active zone set. The zoning configuration values (autosave, default visibility) remain unchanged.

Notes The following tables specify the various factory default settings:

Table B-2. Switch Configuration Defaults

Parameter	Default
Admin State	Online
Broadcast Enable	True
InbandEnable	True
Domain ID	1
Domain ID Lock	False
Symbolic Name	SANbox2
R_T_TOV	100
R_A_TOV	10000
E_D_TOV	2000
FS_TOV	5000
DS_TOV	5000
Principal Priority	254
System Description	Undefined
Configuration Last Saved By	Initial
Configuration Last Saved On	Initial

Table B-3. Port Configuration Defaults

Parameter	Default
Admin State	Online
Link Speed	Auto
Port Type	GL
TL_Port Mode	TLTargetMode
ISL Security	Any
Symbolic Name	Port

Table B-3. Port Configuration Defaults (Continued)

Parameter	Default
ALFairness	False
ARB_FF	False
InteropCredit	0
ExtCredit	0
FanEnable	True
LCFEnable	False
MFSEnable	True
MFS_TOV	10
MSEnable	True
NoClose	False
IOStreamGuard	Disabled
VIEnable	False
CheckAlps	False

Table B-4. Alarm Threshold Configuration Defaults

Parameter	Default
ThresholdMonitoringEnabled	False
CRCErrorsMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 25 1 10
DecodeErrorsMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 25 0 10
ISLMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 2 0 10

Table B-4. Alarm Threshold Configuration Defaults (Continued)

Parameter	Default
LoginMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10
LogoutMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10
LOSMonitoringEnabled	True
RisingTrigger	100
FallingTrigger	5
SampleWindow	10

Table B-5. SNMP Configuration Defaults

Parameter	Default
Contact	Undefined
Location	Undefined
Description	Undefined
Trap [1-5] Address	10.0.0.254
Trap [1-5] Port	Undefined
Trap [1-5] Severity	Warning
Trap [1-5] Enabled	False
ObjectID	1.3.6.1.4.1.1663.1.1.1.1.12
AuthFailureTrap	False

Table B-6. System Configuration Defaults

Parameter	Default
Ethernet Network IP Address	10.0.0.1
Ethernet Network IP Mask	255.0.0.0
Ethernet Gateway Address	10.0.0.254
Ethernet Network Discovery	Static
Admin Timeout	30 minutes
Security Enabled	False
Local Log Enabled	True
Remote Log Enabled	False
Remote Log Host IP Address	Undefined

Set Command

Sets a variety of switch, I/O blade, and port parameters.

Authority Admin for all keywords except Alarm Clear, Beacon, and Pagebreak which are available with User authority.

Syntax

set
alarm clear
beacon [state]
blade [slot_number] [state]
config [option]
log [option]
pagebreak [state]
port [option]
setup [option]
switch [state]

Keywords

alarm clear
Clears the alarm log. This keyword is available with User authority.

beacon [state]
Enables or disables the flashing of the Port Status LEDs according to [state]. This keyword is available with User authority. [state] can be one of the following:

on
Enables the flashing beacon.

off
Disables the flashing beacon.

blade [slot_number] [state]
Temporarily changes the administrative state given by [state] for all ports on the I/O or cross-connect blade occupying the slot given by [slot_number]. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a switch configuration. [slot_number] is a number in the ranges 1–4 and 6–9. [state] can be one of the following:

online
Places the I/O blade and its ports online.

offline
Places the I/O blade and its ports offline.

diagnostics
Prepares the I/O blade and its ports for testing.

down
Disables the I/O blade and its ports.

config [option]
Sets switch, blade, port, alarm threshold, and zoning configuration parameters. Refer to the ”Set Config Command” on page B-27.

log [option]
Specifies the type of entries to be entered in the event log. Refer to the ”Set Log Command” on page B-35.

pagebreak [state]
Specifies how much information is displayed on the screen at a time according to the value given by [state]. This keyword is available with User authority. [state] can be one of the following:

on
Limits the display of information to 20 lines at a time. The page break functions affects the following commands: Alias (List, Members), Show (Alarm, Log), Zone (List, Members), Zoneset (List, Zones), Zoning (Active, List).

off
Allows continuous display of information without a break.

port [option]
Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. Refer to the ”Set Port Command” on page B-38.

setup [option]
Changes SNMP and system configuration settings. Refer to the ”Set Setup Command” on page B-40.

switch [state]
Temporarily changes the administrative state for all ports on the switch to the state given by [state]. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a switch configuration. [state] can be one of the following:

online
Places all ports online

offline
Places all ports offline.

diagnostics
Prepares all ports for testing.

Set Config Command

Sets switch, port, alarm threshold, and zoning configuration parameters.

Authority Admin authority and a Config Edit session

Syntax

set config
blade *[slot_number]*
port *[port_number]*
ports *[port_number]*
switch
threshold
zoning

Keywords

blade *[slot_number]*
Initiates an edit session in which to change configured administrative state for an I/O or cross-connect blade occupying the slot given by [slot_number]. If you omit [slot_number], the system begins with slot 1 and proceeds in order through slot 12. Slots 1–4 and 6–9 are I/O blades; slots 11–12 are cross-connect blades. Enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to cancel the configuration for one blade, or “qq” to cancel the configuration for all blades.

port *[port_number]*
Initiates an edit session in which to change configuration parameters for the port number given by [port_number]. If you omit [port_number], the system begins with port 0 and proceeds in order through the last port. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to cancel the configuration for one port, or “qq” to cancel the configuration for all ports. Table B-7 describes the port parameters.

ports *[port_number]*
Initiates an editing session in which to change configuration parameters for all ports based on the configuration for the port given by [port_number]. If you omit [port_number], port 0 is used. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to cancel the configuration. Table B-7 describes the port parameters.

Table B-7. Set Config Port Parameters

Parameter	Description
AdminState	Port administrative state: online, offline, diagnostics, or down.
LinkSpeed	1Gb/sec or 2 Gb/sec
PortType	Type of port
TLPortMode	Configures a TL_Port for a loop of private target or initiator devices.

Table B-7. Set Config Port Parameters (Continued)

Parameter	Description
ISLSecurity	E_Port security. Determines which switches a port will establish a link with. ■ Any - link with any FC-SW-2 compliant switch. ■ Ours - link only with an FC-SW-2 compliant QLogic switch. ■ None - reject the link.
SymbolicPortName	Descriptive name
ALFairness	Arbitration loop fairness. Enables (True) or disables (False) the switch's priority to arbitrate on the loop.
ARB_FF	Use ARB_FF instead of idles on loop FCAL option
InteropCredit	Interoperability credit. The number of buffer-to-buffer credits per port. 0 means the default (12) is unchanged.
ExtCredit	Extended credits. The number of port buffer credits that this port can acquire from donor ports.
FANEnable	Fabric address notification. Enables (True) or disables (False) the communication of the FL_Port address, port name, and node name to the logged-in NL_Port.
LCFEnable	Link control frame preference, R_CTL = 0xC
MFSEnable	Multi-Frame Sequence bundling
MFS_TOV	MFS limit for camp on
MSEnable	Management Server enable on this port
NoClose	Don't close unless another device arbitrates
I/O Stream Guard	Enables or disables the suppression of RSCN messages
VIEnable	Enable VI preference routing
CheckAlps	Close before sending frames to new target

switch
Initiates an editing session in which to change switch configuration settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table B-8. Set Config Switch Parameters

Parameter	Description
AdminState	Switch administrative state: online, offline, or diagnostics
BroadcastEnabled	Enables (True) or disables (False)) forwarding of broadcast frames.
InbandEnabled	Enables (True) or disables (False) the ability to manage the switch over an ISL.
DefaultDomainID	Default domain ID setting
DomainIDLock	Prevents (True) or allows (False) dynamic reassignment of the domain ID.
SymbolicName	Descriptive name
R_T_TOV	Receiver Transmitter Timeout Value. Specifies the number of milliseconds a port is to wait to receive a response from another port. The default is 100.
R_A_TOV	Resource Allocation Timeout Value. The number of milliseconds the switch waits to allow two ports to allocate enough resources to establish a link. The default is 10000.
E_D_TOV	Error Detect Timeout Value. The number of milliseconds a port is to wait for errors to clear. The default is 2000.
FS_TOV	Fabric Stability Timeout Value. The default is 5000 msec.
DS_TOV	Distributed Services Timeout Value (Management Server, Name Server). The default is 5000 msec.
PrincipalPriority	The priority used in the FC-SW-2 principal switch selection algorithm. 1 is high, 255 is low.
ConfigDescription	The name for the configuration. The default is undefined.

threshold
Initiates a configuration session by which to generate and log alarms for selected events. The system displays each event, its thresholds, and sampling interval one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. These parameters must be saved in a configuration and activated before they will take effect. Refer to the "Config Command" on page B-7 for information about saving and activating a configuration. Table B-9 describes the Set Config Threshold parameters. The switch will down a port if an alarm condition is not cleared within three consecutive sampling intervals (by default 30 seconds). An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling threshold.

Table B-9. Set Config Threshold Parameters

Parameter	Description
Threshold Monitoring Enabled	Master enable/disable parameter for all events. Enables (True) or disables (False - the default) the generation of all enabled event alarms.
CRCErrorsMonitoringEnabled DecodeErrorsMonitoringEnabled ISLMonitoringEnabled LoginMonitoringEnabled LogoutMonitoringEnabled LOSMonitoringEnabled	The event type enable/disable parameter. Enables (True) or disables (False) the generation of alarms for each of the following events: ■ CRC errors ■ Decode errors ■ ISL connection count ■ Login errors ■ Logout errors ■ Loss-of-signal errors
Rising Trigger	The event count above which a rising threshold alarm is logged. The switch will not generate another rising threshold alarm for that event until the count descends below the falling threshold and again exceeds the rising threshold.
Falling Trigger	The event count below which a falling threshold alarm is logged. The switch will not generate another falling threshold alarm for that event until the count exceeds the rising threshold and descends again below the falling threshold.
Sample Window	The period of time in seconds in which to count events.

zoning
Initiates an editing session in which to change switch zoning attributes. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table B-10. Set Config Zoning Parameters

Parameter	Description
AutoSave	Enables (On) or disables (Off) the saving of changes to active zone set in the switch's permanent memory. Changes are always saved in the switch's temporary memory.
Default	Enables (All) or disables (None) communication among the switch's ports/ devices and the fabric in the absence of an active zone set.

Examples

The following is an example of the Set Config Blade command:

```
SANbox2-64 108 (admin-config) #> set config blade 1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the default value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'qq' and the ENTER key to do so.

  Configuring Blade in Slot Number:  1
  ---------------------------------

  AdminState    (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Port command:

```
SANbox2-64 N108 #> admin start
SANbox2-64 N108 (admin) #> config edit
SANbox2-64 N108 (admin-config) #>> set config port 1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  1
  ------------------------

  AdminState    (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online]
  LinkSpeed     (1=1Gb/s, 2=2Gb/s, 3=Auto)                   [Auto  ]
  PortType      (TL / GL / G / F / FL / Donor)               [GL    ]
  TLPortMode    (1=TLTargetMode, 2=TLInitiatorMode)          [TLInitiatorMode]
  ISLSecurity   (Any /  Ours / None)                         [Any   ]
  SymPortName   (string, max=32 chars)                       [Port2 ]
  ALFairness    (True / False)                               [False ]
  ARB_FF        (True / False)                               [False ]
  InteropCredit (decimal value, 0-255)                       [0     ]
  ExtCredit     (decimal value, 0-65535)                     [0     ]
  FANEnable     (True / False)                               [True  ]
  LCFEnable     (True / False)                               [False ]
  MFSEnable     (True / False)                               [False ]
  MFS_TOV       (decimal value, 10-20480 msec)               [640   ]
  MSEnable      (True / False)                               [True  ]
  NoClose       (True / False)                               [False ]
  I/O Stream Guard -
              (Suppress RSCN)(Enable / Disable)            [Disable]
  VIEnable      (True / False)                               [False ]
  CheckAlps     (True / False)                               [False ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Switch command:

```
SANbox2-64 N108 #> admin start
SANbox2-64 N108 (admin) #> config edit
SANbox2-64 N108 (admin-config) #>> set config switch

  A list of attributes with formatting and default values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  AdminState         (1=Online, 2=Offline, 3=Diagnostics) [Online       ]
  InbandEnabled      (True / False)                       [False        ]
  BroadcastEnable    (True / False)                       [False        ]
  DefaultDomainID    (decimal value, 1-239)               [11           ]
  DomainIDLock       (True / False)                       [True         ]
  SymbolicName       (string, max=32 chars)               [SANbox2-64 108]
  R_T_TOV            (decimal value, 1-1000 msec)         [100          ]
  R_A_TOV            (decimal value, 100-100000 msec)     [10000        ]
  E_D_TOV            (decimal value, 10-20000 msec)       [2000         ]
  FS_TOV             (decimal value, 100-100000 msec)     [5000         ]
  DS_TOV             (decimal value, 100-100000 msec)     [5000         ]
  PrincipalPriority  (decimal value, 1-255)               [254          ]
  ConfigDescription  (string, max=32 chars)               [SANbox2-64 FC Switch]
```

The following is an example of the Set Config Zoning command.

```
SANbox2-64 N108 #> admin start
SANbox2-64 N108 (admin) #> config edit
SANbox2-64 N108 (admin-config) #>> set config zoning

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  AutoSave      (True / False)  [True]
  Default       (All / None)    [All ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Threshold command:

```
SANbox2-64 N108 (admin-config) #>>set config threshold
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  ThresholdMonitoringEnabled       (True / False)               [False]

  CRCErrorsMonitoringEnabled       (True / False)               [True ]
    RisingTrigger                  (decimal value, 1-1000)      [25   ]
    FallingTrigger                 (decimal value, 0-1000)      [1    ]
    SampleWindow                   (decimal value, 1-1000 sec)  [10   ]

  DecodeErrorsMonitoringEnabled    (True / False)               [True ]
    RisingTrigger                  (decimal value, 1-1000)      [200  ]
    FallingTrigger                 (decimal value, 0-1000)      [0    ]
    SampleWindow                   (decimal value, 1-1000 sec)  [10   ]

  ISLMonitoringEnabled             (True / False)               [True ]
    RisingTrigger                  (decimal value, 1-1000)      [2    ]
    FallingTrigger                 (decimal value, 0-1000)      [0    ]
    SampleWindow                   (decimal value, 1-1000 sec)  [10   ]

  LoginMonitoringEnabled           (True / False)               [True ]
    RisingTrigger                  (decimal value, 1-1000)      [5    ]
    FallingTrigger                 (decimal value, 0-1000)      [1    ]
    SampleWindow                   (decimal value, 1-1000 sec)  [10   ]

  LogoutMonitoringEnabled          (True / False)               [True ]
    RisingTrigger                  (decimal value, 1-1000)      [5    ]
    FallingTrigger                 (decimal value, 0-1000)      [1    ]
    SampleWindow                   (decimal value, 1-1000 sec)  [10   ]

  LOSMonitoringEnabled             (True / False)               [True ]
    RisingTrigger                  (decimal value, 1-1000)      [100  ]
    FallingTrigger                 (decimal value, 0-1000)      [5    ]
    SampleWindow                   (decimal value, 1-1000 sec)  [10   ]
```

Set Log Command

Specifies the type of entries to be entered in the event log. The log is a storage file contained on the switch. The log can hold a maximum of 200 entries. When the log becomes full, the entries are replaced, starting with the oldest entry, to produce a list of the last 200 events which occurred. Log entries are created for ports, components, and event severity levels.

Authority Admin

Syntax

set log
archive
clear
component [list]
level [level]
port [port_list]
restore
save
start (default)
stop

Keywords

archive
Archives the log entries to a file on the switch named *logfile that* can be downloaded from the switch using FTP. To download the log file, open an FTP session, log in with account name/password of “images” for both, and type “get logfile”.

clear
Clears all log entries.

component [list]
Specifies one or more components to monitor for events. Use spaces to delimit values in the list. Choose one or more of the following values:

All
Monitors all components. To maintain optimal switch performance, do not use this setting with the Level keyword set to Info.

Blade
Monitors modular circuit boards in cabinets, racks, and high-port-count switches.

Chassis
Monitors chassis hardware components such as fans and power supplies.

Eport
Monitors all E_Ports.

Mgmtserver
Monitors management server status.

Nameserver
Monitors name server status.

None
Monitor none of the component events.

Other
Monitors other miscellaneous events.

Port
Monitors all port events

Switch
Monitors switch management events.

Zoning
Monitors zoning conflict events.

level [level]
Specifies the severity level given by [level] to use in monitoring events for the specified components or ports. [level] can be one of the following values:

Critical
Monitors critical events.

Warn
Monitors warning events.

Info
Monitors informational events. To maintain optimal switch performance, do not use this setting with the Component keyword set to All.

None
Monitors none of the severity levels.

port [port_list]
Specifies one or more ports to monitor for events. Choose one of the following values:

[port_list]
Specifies port or ports to monitor. Use spaces to delimit values in the list. Ports are numbered beginning with 0.

All
Specifies all ports.

None
Disables monitoring on all ports.

restore
Returns the port, component, and level settings to the default values.

save
Saves the log settings for the component, level, and port. These settings remain in effect after a switch reset. The log settings can be viewed using the Show Log Settings command. To export log entries to a file, use the Set Log Archive command.

start
Starts the logging of events based on the Port, Component, and Level keywords assigned to the current configuration. The logging continues until you enter the Set Log Stop command.

stop
Stops logging of events.

Notes To maintain optimal switch performance, do not set the Component keyword to All and the Level keyword to Info at the same time.

Set Port Command

Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. This command also clears port counters.

Authority Admin

Syntax

set port [port_number]
bypass [alpa]
clear
enable
speed [transmission_speed]
state [state]

Keywords

[port_number]
Specifies the port. Ports are numbered beginning with 0.

bypass [alpa]
Sends a Loop Port Bypass (LPB) to a specific Arbitrated Loop Physical Address (ALPA) or to all ALPAs on the arbitrated loop. [alpa] can be a specific ALPA or the keyword ALL to choose all ALPAs.

clear
Clears the counters on the specified port.

enable
Sends a Loop Port Enable (LPE) to all ALPAs on the arbitrated loop.

speed [transmission_speed]
Specifies the transmission speed for the specified port. Choose one of the following port speed values:

1Gb/s
One gigabit per second.

2Gb/s
Two gigabits per second.

Auto
The port speed is automatically detected.

state [state]
Specifies the administrative state for the specified port. Choose one of the following port state values:

Online
Places the port online.

Offline
Places the port offline.

Diagnostics
Prepares the port for testing.

Down
Disables the port.

Set Setup Command

Changes SNMP and system configuration settings. The switch maintains one SNMP configuration and one system configuration.

Authority Admin

Syntax **set setup**
snmp
system

Keywords **snmp**
Prompts you in a line-by-line fashion to change SNMP configuration settings. Table B-11 describes the SNMP fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table B-11. SNMP Configuration Settings

Entry	Description
Contact	Specifies the name of the person to be contacted to respond to trap events. The default is undefined.
Location	Specifies the name of the switch location. The default is undefined.
Trap [1-5] Address	Specifies the workstation IP address to which SNMP traps are sent. The default is 10.0.0.254.
Trap [1-5] Port	Specifies the workstation port to which SNMP traps are sent.
Trap [1-5] Severity	Specifies the severity level to use when monitoring trap events. The default is Warning
Trap [1-5] Enabled	Specifies whether traps (event information) are enabled or disabled (default).
ReadCommunity	Read community password that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “public”.
WriteCommunity	Write community password that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “private”.

Table B-11. SNMP Configuration Settings

Entry	Description
TrapCommunity	Trap community password that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “public”.
AuthFailureTrap	Enables or disables the reporting of SNMP authentication failures. If enabled, a notification trap is sent when incorrect community string values are used. The default is "False".

system
Prompts you in a line-by-line fashion to change system configuration settings. Table B-12 describes the system configuration fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table B-12. System Configuration Settings

Entry	Description
Eth0NetworkAddress	Internet Protocol (IP) address for the Ethernet port.
Eth0NetworkMask	Subnet mask address for the Ethernet port.
Eth0GatewayAddress	IP address gateway.
Eth0NetworkDiscovery	Boot Method (1 - Static, 2 - Bootp, 3 - DHCP, 4 - RARP)
AdminTimeout	Specifies the amount of time in minutes the switch waits before terminating an idle Admin session. Zero (0) disables the time out threshold. The default is 30, the maximum is 1440.
SecurityEnabled	Enables or disables the enforcement of account names and passwords.
LocalLogEnabled	Enables or disables the saving of log information on the switch.
RemoteLogEnabled	Enables (True) or disables (False) the recording of the switch event log on a remote host that supports the syslog protocol.
RemoteLogHost IPAddress	The IP address of the remote host that will receive the switch event log information.

Notes The two components of security are user authentication and fabric security. The user must be authenticated before gaining access to a switch. If an invalid account name/password combination is entered, that user can not access the switch, and thus can not gain access to the fabric. If security is enabled (True) and a valid account name/password combination is entered, that user can access the switch but can not execute any command that exceeds their authority (privileges) level. If security is disabled (False) and a valid account name/password combination is entered, that user has access to all switches in the fabric and can execute all commands (both user and admin), regardless of their authority (privileges) level.

Examples The following is an example of the Set Setup SNMP command:

```
SANbox2-64 N108 #> admin start
SANbox2-64 N108 (admin) #> set setup snmp
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Trap Severity Options
  ---------------------
  unknown, emergency, alert, critical, error, warning, notify, info, debug, mark

  Contact             (string, max=32 chars)       [<sysContact undefined> ]
  Location            (string, max=32 chars)       [<sysLocation undefined>]
  Trap1Address        (dot-notated IP Address)     [10.0.0.254             ]
  Trap1Port           (decimal value)              [162                    ]
  Trap1Severity       (see allowed options above)  [warning                ]
  Trap1Enabled        (True / False)               [False                  ]
  Trap2Address        (dot-notated IP Address)     [0.0.0.0                ]
  Trap2Port           (decimal value)              [162                    ]
  Trap2Severity       (see allowed options above)  [warning                ]
  Trap2Enabled        (True / False)               [False                  ]
  Trap3Address        (dot-notated IP Address)     [0.0.0.0                ]
  Trap3Port           (decimal value)              [162                    ]
  Trap3Severity       (see allowed options above)  [warning                ]
  Trap3Enabled        (True / False)               [False                  ]
  Trap4Address        (dot-notated IP Address)     [0.0.0.0                ]
  Trap4Port           (decimal value)              [162                    ]
  Trap4Severity       (see allowed options above)  [warning                ]
  Trap4Enabled        (True / False)               [False                  ]
  Trap5Address        (dot-notated IP Address)     [0.0.0.0                ]
  Trap5Port           (decimal value)              [162                    ]
```

```
  Trap5Severity       (see allowed options above)  [warning               ]
  Trap5Enabled        (True / False)               [False                 ]
  ReadCommunity       (string, max=32 chars)       [public                ]
  WriteCommunity      (string, max=32 chars)       [private               ]
  TrapCommunity       (string, max=32 chars)       [public                ]
  AuthFailureTrap     (True / False)               [False                 ]

  Do you want to save and activate this snmp setup? (y/n) [n]
```

The following is an example of the Set Setup System command:

```
SANbox2-64 N108 #> admin start
SANbox2-64 N108 (admin) #> set setup system

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Eth0NetworkAddress    (dot-notated IP Address)            [10.20.11.108 ]
  Eth0NetworkMask       (dot-notated IP Address)            [255.255.252.0]
  Eth0GatewayAddress    (dot-notated IP Address)            [10.20.8.254  ]
  Eth0NetworkDiscovery  (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp) [Static       ]
  AdminTimeout          (dec value 0-1440 minutes, 0=never) [30           ]
  SecurityEnabled       (True / False)                      [False        ]
  LocalLogEnabled       (True / False)                      [True         ]
  RemoteLogEnabled      (True / False)                      [False        ]
  RemoteLogHostAddress  (dot-notated IP Address)            [10.0.0.254   ]
```

Show Command

Displays fabric, switch, and port operational information.

Authority User

Syntax **show**

about
alarm
blade
broadcast
chassis
config [option]
domains
donor
fabric
interface
log *[option]*
lsdb
mem [count]
ns *[option]*
pagebreak
panel
perf *[option]*
port *[port_number]*
post log
setup [option]
slot *[slot_number]*
steering *[domain_id]*\
support
switch
topology
users
version

Keywords **about**
Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the Version keyword.

alarm
Displays the last 200 alarm entries.

blade
Displays information about the I/O blades and cross-connect modules.

broadcast
Displays the broadcast tree information and all ports that are currently transmitting and receiving broadcast frames.

chassis
Displays chassis component status and temperature.

config [option]
Displays switch and port configuration attributes. Refer to the "Show Config Command" on page B-55.

domains
Displays list of each domain and its worldwide name in the fabric.

donor
Displays list of current donor configuration for all ports.

fabric
Displays list of each domain, fabric ID, worldwide name, node IP address, and port IP address.

interface
Displays the status of the active network interfaces.

log *[option]*
Displays log entries. Refer to the "Show Log Command" on page B-58.

lsdb
Displays Link State database information.

mem [count]
Displays information about memory activity for the number of seconds given by [count]. If you omit [count], the value 1 is used. Displayed memory values are in 1K block units.

Note: This keyword will display memory activity updates until [count] is reached – it cannot be interrupted. Therefore, avoid using large values for [count].

ns *[option]*
Displays name server information for the specified [option]. If you omit [option], name server information for the local domain ID is displayed. [option] can have the following values:

all
Displays name server information for all switches and ports.

[domain_id]
Displays name server information for the switch given by [domain_id]. [domain_id] is a switch domain ID.

[port_id]
Displays name server information for the port given by [port_id]. [port_id] is a port Fibre Channel address.

pagebreak
Displays the current pagebreak setting. The pagebreak setting limits the display of information to 20 lines (On) or allows the continuous display of information without a break (Off).

panel
Displays the hardware configuration and port mapping for a SANbox2-64 switch. The representation of the faceplate indicates power supply modules (PS), I/O blades (IO), and CPU module (CPU).

perf *[option]*
Displays performance information for all ports. Refer to the "Show Perf Command" on page B-60.

port *[port_number]*
Displays operational information for the port given by [port_number]. Ports are numbered beginning with 0. If the port number is omitted, information is displayed for all ports. Table B-13 describes the port parameters.

Table B-13. Show Port Parameters

Entry	Description
AlInit	Incremented each time the port begins AL initialization.
AlInitError	Number of times the port entered initialization and the initialization failed.
ClassXFramesIn	Number of class *x* frames received by this port.
ClassXFramesOut	Number of class *x* frames sent by this port.
ClassXWordsIn	Number of class *x* words received by this port.
ClassXWordsOut	Number of class *x* words sent by this port.
DecodeError	Decoding error detected.
FBusy	Number of times the switch sent a F_BSY because Class 2 frame could not be delivered within ED_TOV time. Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_Port that is preventing delivery of this frame.
Flowerrors	Received a frame when there were no available credits.

Table B-13. Show Port Parameters (Continued)

Entry	Description
FReject	Number of frames from devices that were rejected.
InvalidCRC	Invalid CRC detected.
InvalidDestAddr	Invalid destination address detected.
LIP ALPD ALPS	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.
LIPF7ALPS	This LIP is used to reinitialize the loop. An L_port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.
LIPF8ALPS	This LIP denotes a loop failure detected by the L_port identified by AL_PS.
LIPF7F7	A loop initialization primitive frame used to acquire a valid AL_PA.
LIPF8F7	A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization for a period of time greater than the value of R_T_TOV or by loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established by the time specified by R_T_TOV, a link failure is counted. A link reset is performed after a link failure.
Login	Time when user logged in.
Logout	Time when user logged out.
LoopTimeouts	A two (2) second timeout as specified by FC-AL-2.
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
PrimSeqErrors	Primitive sequence errors detected.

Table B-13. Show Port Parameters (Continued)

Entry	Description
EportConnects	Shows the count of the number of times an E_Port connected through ISL negotiation.
RxLinkResets	Number of link reset primitives received from an attached device.
RxOfflineSeq	Number of offline sequences received. An OLS is issued for link initialization, a Receive & Recognize Not_Operational (NOS) state, or to enter the offline state.
TotalErrors	Total number of errors detected.
TotalLIPsRecvd	Number of loop initialization primitive frames received by this port.
TotalLinkResets	Total number of link reset primatives.
TotalOfflineSeq	Total number of Offline Sequences issued by this port.
TotalRxFrames	Total number of frames received by this port.
TotalRxWords	Total number of words received by this port.
TotalTxFrames	Total number of frames issued by this port.
TotalTxWords	Total number of words issued by this port.
TxLinkResets	Number of Link Resets issued by this port.
TxOfflineSeq	Total number of Offline Sequences issued by this port.
TxWait	Time waiting to transmit when blocked with no credit. Measured in FC Word times.

post log
Displays the Power On Self Test (POST) log which contains results from the POST.

setup [option]
Displays setup attributes for the system, SNMP, and the switch manufacturer. Refer to the "Show Setup Command" on page B-62.

slot *[slot_number]*
Displays the hardware attributes for the slot on a SANbox2-64 switch given by [slot_number]. [slot_number] can be 0–10. If you omit [slot_number], the hardware configuration for all slots is displayed.

steering *[domain_id]*
Displays the routes that data takes to the switch given by [domain_id]. If you omit [domain_id], the system displays routes for all switches in the fabric.

support
Executes a series of commands that display a complete description of the switch, its configuration, and operation. The display can be captured from the screen and used for diagnosing problems. This keyword is intended for use at the request of your authorized maintenance provider. The commands that are executed include the following:

- Date
- Alias List
- Config List
- Date
- History
- Ps
- Show (About, Alarm, Backtrace, Chassis, Config Port, Config Switch, Dev, Dev Settings, Domains, Donor, Fabric, Log, Log Settings, Lsdb, Mem, Ns, Perf, Port, Setup Mfg, Setup Snmp, Setup System, Steering, Switch, Topology, Users)
- Uptime
- User Accounts
- Whoami
- Zoneset (Active, List)
- Zoning (History, Limits, List)

switch
Displays switch operational information.

topology
Displays all connected devices.

users
Displays a list of logged-in users. This is equivalent to the User List command.

version
Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the About keyword.

Examples

The following is an example of the Show Blade command:

```
SANbox2-64 N108 #> show blade
  Blade  Slot   Port  Admin         Oper         Diag         Temp        Credit
  Type   Number Range State        State        Status       Status      Pool
  -----  ------ ----- -----        -----        ------       ------      ------
  IO-0   1       0-7  Online       Online       Compromised  Normal      0
  IO-1   2       8-15 Online       Online       Passed       Normal      0
  IO-2   3      16-23 Online       NotInstalled NotInstalled Normal      0
  IO-3   4      24-31 Online       NotInstalled NotInstalled Normal      0
  IO-4   6      32-39 Online       Online       Compromised  Normal      0
  IO-5   7      40-47 Online       Online       Passed       Normal      0
  IO-6   8      48-55 Online       NotInstalled NotInstalled Normal      0
  IO-7   9      56-63 Online       NotInstalled NotInstalled Normal      0
  CC-0   11       *   Online       Online       Passed       Normal      *
  CC-1   12       *   Online       Online       Passed       Normal      *
```

The following is an example of the Show Chassis command:

```
SANbox2-64 N108 #> show chassis

  Chassis Information
  -------------------
  FanStatus (1)                   Good
  FanStatus (2)                   Good
  FanStatus (3)                   Good
  PowerSupplyStatus (1)           NotInstalled
  PowerSupplyStatus (2)           NotInstalled
  HeartBeatCode                   1
  HeartBeatStatus                 Normal

  User Ports Map
  --------------
  (displays Non Real-Time data for slot # and blade type-instance)

  SL#0  SL#1  SL#2  SL#3  SL#4  SL#5  SL#6  SL#7  SL#8  SL#9  SL#10
  PS-0  IO-0  IO-1  IO-2  IO-3  CPU-0 IO-4  IO-5  IO-6  IO-7  PS-1
  ------------------------------------------------------------------
   *     0     8     16    24    *     32    40    48    56    *
   *     1     9     17    25    *     33    41    49    57    *
   *     2     10    18    26    *     34    42    50    58    *
   *     3     11    19    27    *     35    43    51    59    *
   *     4     12    20    28    *     36    44    52    60    *
   *     5     13    21    29    *     37    45    53    61    *
```

```
  *     6     14    22    30    *     38    46    54    62    *
  *     7     15    23    31    *     39    47    55    63    *
```

The following is an example of the Show Fabric command:

```
SANbox2-64 N108 #> show fabric

Switch     ID     WWN                       Eth0IPAddress
------     --     ---                       -------------
97 (0x61)  fffc61 10:00:00:c0:dd:00:bc:08  10.20.11.107
98 (0x62)  fffc62 10:00:00:60:69:20:4c:a2  10.20.11.156
99 (0x63)  fffc63 10:00:00:c0:dd:00:71:a0  10.20.11.104
100 (0x64) fffc64 10:00:00:c0:dd:00:90:29  10.20.11.97
101 (0x65) fffc65 10:00:00:c0:dd:00:91:11  10.20.11.108
102 (0x66) fffc66 10:00:00:c0:dd:00:90:85  10.20.11.24
```

The following is an example of the Show Panel command:

```
SANbox2-64 N108 #> show panel

  User Ports Map
  --------------
  (displays Non Real-Time data for slot # and blade type-instance)

  SL#0  SL#1  SL#2  SL#3  SL#4  SL#5  SL#6  SL#7  SL#8  SL#9  SL#10
  PS-0  IO-0  IO-1  IO-2  IO-3  CPU-0 IO-4  IO-5  IO-6  IO-7  PS-1
  ------------------------------------------------------------------
   *     0     8     16    24    *     32    40    48    56    *
   *     1     9     17    25    *     33    41    49    57    *
   *     2     10    18    26    *     34    42    50    58    *
   *     3     11    19    27    *     35    43    51    59    *
   *     4     12    20    28    *     36    44    52    60    *
   *     5     13    21    29    *     37    45    53    61    *
   *     6     14    22    30    *     38    46    54    62    *
   *     7     15    23    31    *     39    47    55    63    *
```

The following is an example of the Show Port command:

```
SANbox2-64 N108 #> show port 3

  Port Number: 3
  ------------
  AdminState       Online              PortID           650300
  AsicNumber       0                   PortWWN          20:03:00:c0:dd:00:91:11
  AsicPort         3                   RunningType      Unknown
  ConfigType       GL                  SFPPartNumber    PL-XPL-00-S23-24
  DiagStatus       Passed              SFPRevision
  EpConnState      None                SFPType          100-M5-SN-I
  EpIsoReason      NotApplicable       SFPVendor        PICOLIGHT
  LinkSpeed        Auto                SFPVendorID      00850400
  LinkState        Inactive            SymbolicName     Port3
  LoginStatus      NotLoggedIn         SyncStatus       SyncLost
  MaxCredit        12                  XmitterEnabled   True
  OperationalState Offline

  ALInit          1         FlowErrors      0         PrimSeqErrors   0
  ALInitError     0         FReject         0         RxLinkResets    0
  Class2FramesIn  0         InvalidCRC      0         RxOfflineSeq    0
  Class2FramesOut 0         InvalidDestAddr 0         TotalErrors     0
  Class2WordsIn   0         LIP_AL_PD_AL_PS 0         TotalLIPsRecvd  0
  Class2WordsOut  0         LIP_F7_AL_PS    0         TotalLinkResets 0
  Class3FramesIn  0         LIP_F7_F7       0         TotalOfflineSeq 2
  Class3FramesOut 0         LIP_F8_AL_PS    0         TotalRxFrames   0
  Class3Toss      0         LIP_F8_F7       0         TotalRxWords    0
  Class3WordsIn   0         LinkFailures    0         TotalTxFrames   0
  Class3WordsOut  0         Login           0         TotalTxWords    0
  DecodeErrors    0         Logout          0         TxLinkResets    0
  EpConnects      0         LoopTimeouts    0         TxOfflineSeq    2
  FBusy           0         LossOfSync      0         TxWaits         0
```

The following is an example of the Show Slot command:

```
SANbox2-64 N108 #> show slot

  Slot   Blade  Port  Blade        Diag          Temp        Credit
  Number Type   Range Status       Status        Status      Pool
  ------ -----  ----- ------       ------        ------      ------
  0      PS-0     *   NotInstalled Passed        Normal      *
  1      IO-0    0-7  Good         Compromised   Normal      0
  2      IO-1    8-15 Good         Passed        Normal      0
```

```
3      IO-2     -   NotInstalled NotInstalled  Normal      0
4      IO-3     -   NotInstalled NotInstalled  Normal      0
5      CPU-0    *   Good         Passed        Normal      *
6      IO-4   32-39 Good         Compromised   Normal      0
7      IO-5   40-47 Good         Passed        Normal      0
8      IO-6     -   NotInstalled NotInstalled  Normal      0
9      IO-7     -   NotInstalled NotInstalled  Normal      0
10     PS-1     *   NotInstalled Passed        Normal      *
11     CC-0     *   Good         Passed        Normal      *
12     CC-1     *   Good         Passed        Normal      *
```

The following is an example of the Show Switch command:

```
SANbox2-64 N108 #> show switch

Switch Information
------------------
SymbolicName                     SANbox2-64 N108
SwitchWWN                        10:00:00:c0:dd:00:91:11
SwitchType                       SANbox2-64
PROMVersion                      V1.4-1-0   (Wed Jul 31 03:53:08 2002)
DomainID                         101 (0x65)
FirstPortAddress                 650000
FlashSize - MBytes               128
LogLevel                         Info
MaxPorts                         64
NumberOfResets                   155
ReasonForLastReset               NormalReset
SWImageVersion (1) - build date  V1.4-7-7   (Wed Jul 31 03:53:08 2002)
SWImageVersion (2) - build date  V1.4-7-6   (Wed Jul 31 13:44:32 2002)
ActiveConfiguration              config8
ActiveSWImage                    1
AdminState                       Online
AdminModeActive                  False
BeaconOnStatus                   False
OperationalState                 Online
PrincipalSwitchRole              False
SwitchDiagnosticsStatus          Compromised
```

The following is an example of the Show Topology (for Port #1) command:

```
SANbox2-64 N108 #> show topology 1

  Local Link Information
  ----------------------

  PortNumber 1
  PortID     650100
  PortWWN    20:01:00:c0:dd:00:91:11
  PortType   F

  Remote Link Information
  -----------------------

  Device 0

    PortID      650100
    PortWWN     10:00:00:00:c9:27:23:8b
    NodeWWN     20:00:00:00:c9:27:23:8b
    PortType    N
    Description (NULL)
    IPAddress   0.0.0.0
```

Show Config Command

Displays switch, I/O blade, port, alarm threshold, and zoning attributes for the current configuration.

Authority User

Syntax **show config**
blade *[slot_number]*
port *[port_number]*
switch
threshold
zoning

Keywords **blade *[slot_number]***
Displays configuration parameters for the I/O blade or cross-connect blade that occupies the slot given by [slot_number]. If you omit [slot_number], the configuration parameters for all I/O and cross-connect blades.

port *[port_number]*
Displays configuration parameters for the port number given by [port_number]. Ports are numbered beginning with 0. If the port value is omitted, all ports are specified.

switch
Displays configuration parameters for the switch.

threshold
Displays alarm threshold parameters for the switch.

zoning
Displays zoning configuration parameters for the switch.

Examples The following is an example of the Show Config Port command:

```
SANbox2-64 N108 #> show config port 3


  Configuration Name: default
  -------------------
  Port Number: 3
  ------------
  AdminState       Online
  LinkSpeed        Auto
  PortType         GL
  TLPortMode       TLInitiatorMode
  ISLSecurity      Any
  SymbolicName     Port4
  ALFairness       False
  ARB_FF           False
  InteropCredit    0
  FanEnable        True
```

```
  ExtCredit        0
  FanEnable        False
  LCFEnable        False
  MFSEnable        False
  MFS_TOV          640
  MSEnable         False
  NoClose          False
  IOStreamGuard    False
  VIEnable         False
  CheckAlps        False
```

The following is an example of the Show Config Switch command:

```
SANbox2-64 N108 #> show config switch

  Configuration Name: default
  -------------------
  Switch Configuration Information
  --------------------------------
  AdminState            Online
  BroadcastEnabled      False
  InbandEnabled         True
  DomainID              11
  DomainIDLock          True
  SymbolicName          bottom switch
  R_T_TOV               100
  R_A_TOV               10000
  E_D_TOV               2000
  FS_TOV                5000
  DS_TOV                5000
  PrincipalPriority     254
  Config Description
  ConfigLastSavedBy     Initial
  ConfigLastSavedOn     Initial
```

The following is an example of the Show Config Zoning command:

```
SANbox2-64 N108 #> show config zoning

 Configuration Name: default
  -------------------
  Zoning Configuration Information
  --------------------------------
  AutoSave              True
  Default               All
```

The following is an example of the Show Config Threshold command:

```
SANbox2-64 N108 #> show config threshold

  Configuration Name: config8
  -------------------

  Threshold Configuration Information
  -----------------------------------
  ThresholdMonitoringEnabled      False
  CRCErrorsMonitoringEnabled      True
    RisingTrigger                 25
    FallingTrigger                1
    SampleWindow                  10
  DecodeErrorsMonitoringEnabled   True
    RisingTrigger                 200
    FallingTrigger                0
    SampleWindow                  10
  ISLMonitoringEnabled            True
    RisingTrigger                 2
    FallingTrigger                0
    SampleWindow                  10
  LoginMonitoringEnabled          True
    RisingTrigger                 5
    FallingTrigger                1
    SampleWindow                  10
  LogoutMonitoringEnabled         True
    RisingTrigger                 5
    FallingTrigger                1
    SampleWindow                  10
  LOSMonitoringEnabled            True
    RisingTrigger                 100
    FallingTrigger                5
    SampleWindow                  10
```

Show Log Command

Displays the contents of the log or the parameters used to create entries in the log. The log contains a maximum of 200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority User

Syntax

show log
- component
- level
- options
- port
- settings

Keywords

component
Displays the components currently being monitored for events.

level
Displays the event severity level needed to create an entry in the log. If the severity level occurs on a port or on a component which is not defined, no entry is made in the log.

options
Displays the options used to set the component and log level attributes.

port
Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but not on a defined port, no entry is made in the log.

settings
Displays the current settings for component, level and port. This command is equivalent to executing the following commands separately: Show Log Component, Show Log Level, and Show Log Port.

Examples The following is an example of the Show Log Component command

```
SANbox2-64 N108 #> show log component

  Current setting(s) for log component: NameServer
```

The following is an example of the Show Log Level command:

```
SANbox2-64 N108 #> show log level

  Current setting(s) for log level: Info
```

The following is an example of the Show Log Options command:

```
SANbox2-64 N108 #> show log options

  Allowed options for ’    level’: Critical,Warn,Info,None

  Allowed options for ’component’: All,None,NameServer,MgmtServer,Zoning,Switch,
Chassis,Blade,Port,Eport,Snmp,Other
```

The following is an example of the Show Log Port command:

```
SANbox2-64 N108 #> show log port

  Current setting(s) for log port: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
```

The following is an example of the Show Log command:

```
[327][Wed Jan 25 09:36:54.860 1989][I][Eport:0xdd00b8b6.304.4 Port: 0/8][Eport
 State = E_A0_GET_DOMAIN_ID]
   [328][Wed Jan 25 09:36:54.860 1989][I][Eport:0xdd00b8b6.304.4 Port: 0/8][FSPF
 PortUp state=0]
   [329][Wed Jan 25 09:36:54.861 1989][I][Eport:0xdd00b8b6.304.4 Port: 0/8][Send
ing init hello]
   [330][Wed Jan 25 09:36:54.861 1989][I][Eport:0xdd00b8b6.304.4 Port: 0/8][Proc
essing EFP, oxid= 0x8]
   [331][Wed Jan 25 09:36:54.861 1989][I][Eport:0xdd00b8b6.304.4 Port: 0/8][Epor
t State = E_A2_IDLE]
   [332][Wed Jan 25 09:36:54.861 1989][I][Eport:0xdd00b8b6.304.4 Port: 0/8][EFP,
 WWN= 0x100000c0dd00b845, len= 0x30]
   [333][Wed Jan 25 09:36:54.864 1989][I][Eport:0xdd00b8b6.304.4 Port: 0/8][Send
ing LSU oxid= 0xc: type= 1]
   [334][Wed Jan 25 09:36:54.864 1989][I][Eport:0xdd00b8b6.304.4 Port: 0/8][Send
 Zone Merge Request]
   [335][Wed Jan 25 09:36:54.865 1989][I][Eport:0xdd00b8b6.304.4 Port: 0/8][LSDB
 Xchg timer set]
   [336][Wed Jan 25 09:36:54.865 1989][I][Eport:0xdd00b8b6.304.4 Port: 0/8][Sett
ing attribute Oper.UserPort.0.8.EpConnState Connected]
```

Show Perf Command

Displays port performance in frames/second and bytes/second. If you omit the keyword, the command displays data transmitted (out), data received (in), and total data transmitted and received in frames/second and bytes per second.

Authority User

Syntax

show perf
- byte
- inbyte
- outbyte
- frame
- inframe
- outframe
- errors

Keywords

byte
Displays continuous performance data in total bytes/second transmitted and received for all ports. Type “q” and press the Enter key to stop the display.

inbyte
Displays continuous performance data in bytes/second received for all ports. Type “q” and press the Enter key to stop the display.

outbyte *[port_number]*
Displays continuous performance data in bytes/second transmitted for the set of 16 ports that include [port_number]. Type “q” and press the Enter key to stop the display.

frame *[port_number]*
Displays continuous performance data in total frames/second transmitted and received for the set of 16 ports that include [port_number]. Type “q” and press the Enter key to stop the display.

inframe *[port_number]*
Displays continuous performance data in frames/second received for the set of 16 ports that include [port_number]. Type “q” and press the Enter key to stop the display.

outframe *[port_number]*
Displays continuous performance data in frames/second transmitted for the set of 16 ports that include [port_number]. Type “q” and press the Enter key to stop the display.

errors *[port_number]*
Displays continuous error counts for the set of 16 ports that include [port_number]. Type “q” and press the Enter key to stop the display.

Examples

The following is an example of the Show Perf Byte command for ports 0–15:

```
SANbox2-64 N108 #> show perf byte

  Displaying bytes/sec data...  (Press 'q' and the ENTER key to stop display)

  0    1    2    3    4    5    6    7    8    9    10   11   12   13   14   15
  ------------------------------------------------------------------------------
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    8K   136M
  0    0    0    0    0    0    0    0    135M 58K  0    0    0    0    7K   135M
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    7K   136M
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    8K   136M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    7K   136M
```

Show Setup Command

Displays the current SNMP and system settings.

Authority User

Syntax **show setup**
mfg
snmp
system

Keywords **mfg**
Displays manufacturing information about the switch.

snmp
Displays the current SNMP settings.

system
Displays the current system settings.

Examples The following is an example of the Show Setup Mfg command:

```
SANbox2 #> show setup mfg
Manufacturing Information
  -------------------------
  BoardSerialNumber      1169582
  BrandName              QLogic
  BuildDate              Unknown
  ChassisPartNumber      Unknown
  ChassisSerialNumber    S02360001
  MACAddress             00:c0:dd:00:72:88
  PlanarPartNumber       Unknown
  SwitchSymbolicName     SANbox2-64
  SwitchWWN              10:00:00:c0:dd:00:72:89
  SystemDescription      SANbox2-64 FC Switch
  SystemObjectID         1.3.6.1.4.1.1663.1.1.1.1.12
```

The following is an example of the Show Setup Snmp command:

```
SANbox2-64 N108 #> show setup snmp
  SNMP Information
  ----------------
  Contact               <sysContact undefined>
  Location              <sysLocation undefined>
  Description           SANBox2 FC Switch
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Enabled          False
  Trap2Address          0.0.0.0
  Trap2Port             162
  Trap2Severity         warning
  Trap2Enabled          False
  Trap3Address          0.0.0.0
  Trap3Port             162
  Trap3Severity         warning
  Trap3Enabled          False
  Trap4Address          0.0.0.0
  Trap4Port             162
  Trap4Severity         warning
  Trap4Enabled          False
  Trap5Address          0.0.0.0
  Trap5Port             162
  Trap5Severity         warning
  Trap5Enabled          False
  ObjectID              1.3.6.1.4.1.1663.1.1.1.1.11
  AuthFailureTrap       False
```

The following is an example of the Show Setup System command:

```
SANbox2-64 N108 #> show setup system

  System Information
  ------------------
  Eth0NetworkAddress       172.22.11.202
  Eth0NetworkMask          255.255.252.0
  Eth0GatewayAddress       172.22.8.254
  Eth0NetworkDiscovery     Static
  AdminTimeout             30
  SecurityEnable           False
  LocalLogEnabled          True
  RemoteLogEnable          False
  RemovteLogHostIPAddress  undefined
```

Shutdown Command

Terminates all data transfers on the switch at convenient points and closes the Telnet session. Always power cycle the switch after entering this command.

Authority Admin

Syntax **shutdown**

Notes Always use this command to effect an orderly shut down before removing power from the switch. Failure to do so could corrupt the flash memory and the switch configuration.

Test Command

Tests I/O blades and ports using internal (SerDes level), external (SFP), and online loopback tests. Internal and external tests require that the I/O blade or the port be placed in diagnostic mode. Refer to the "Set Command" on page B-25 for information about changing the port or I/O blade administrative state. While the test is running, the remaining ports on the switch remain fully operational.

Authority Admin

Syntax

test
port [port_number] [test_type]
blade [slot_number]
cancel
status

Keywords

port [port_number] *[test_type]*
Tests the port given by [port_number] using the test given by [test_type]. If you omit [test_type], Internal is used. [test_type] can have the following values:

internal
Tests the SerDes. This is the default. The port must be in diagnostics mode to perform this test.

external
Tests both the SerDes and SFP. The port must be in diagnostics mode to perform this test, and a loopback plug must be installed in the SFP.

online
Tests one online port.

blade [slot_number]
Tests the ASIC registers and performs an internal SerDes test on all ports on the I/O blade that occupies the slot given by [slot_number]. I/O blade slot numbers are 1–4 and 6–9. The I/O blade must be in diagnostics mode to perform this test.

cancel
Cancels the online test in progress.

status
Displays the status of a test in progress, or if there is no test in progress, the status of the test that was executed last.

Examples To run Internal (SerDes) or External (SFP) port tests, do the following:

1. To start an admin session, enter the following command and press the Enter key.

   ```
   admin start
   ```

2. Place the port in Diagnostics mode, enter the following command (*x* = port number) and press the Enter key.

   ```
   set port x state diagnostics
   ```

3. Insert the loopback plug into the SFP on the selected port.
4. Choose the type of port loopback test to run:
   - To run an internal loopback test, enter the following:

     `test x internal`

   - To run an external loopback test, enter the following command. A loopback plug must be installed for this test to pass.

     `test x external`
5. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload.
6. After the test type has been chosen and the command executed, a message on the screen will appear detailing the test results.
7. After the test is run, put the port back into online state by entering the following command (*x* = port number) and pressing the Enter key.

   `set port x state online`
8. To verify port is back online, enter the following command and press the Enter key. The contents of the AdminState field should display be “Online”.

   `show port x`

The online loopback (node-to-node) test can test only one port at a time, and that port must be online and connected to a remote device. To run the online loopback test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

   `admin start`
2. To run the online loopback test, enter the following command and press the Enter key.

   `test x online`

3. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload. Before running the test, make sure that the device attached to the port can handle the test parameters.

   ```
   SANbox2N107 (admin) #> test x online

   A list of attributes with formatting and current values will
   follow. Enter a new value or simply press the ENTER key to
   accept the default value. If you wish to terminate this
   process before reaching the end of the list press 'q' or 'Q'
   and the ENTER key to do so.

     TestLength    (decimal value, 1-4294967295)   [100    ]
     FrameSize     (decimal value, 36-2148)        [256    ]
     DataPattern   (32-bit hex value or 'Default') [Default]
     StopOnError   (True/False)                    [False  ]
     Do you want to start the test? (y/n) [n]
   ```

4. After all parameter values are defined, press the Y key to start the test.

Uptime Command

Displays the elapsed time since the switch was last reset and reset method.

Authority User

Syntax **uptime**

Examples The following is an example of the Uptime command:

```
SANbox2-64 N108 #> uptime

  Elapsed up time  : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
  Reason last reset: NormalReset
```

User Command

Administers or displays user accounts.

Authority Admin. The List keyword is available with User authority.

Syntax

user
accounts
add
delete [account_name]
list

Keywords

accounts
Displays all user accounts that exist on the switch.

add
Add a user account to the switch. After this command is executed, the administrator will be prompted for the information needed to establish the user account. A switch can have a maximum of 15 user accounts. Account names are limited to 15 characters; passwords are limited to 31 characters.

delete [account_name]
Deletes the account name given by [account_name] from the switch.

list
Displays the list of users currently logged in and their session numbers. Provides the same function as the Show Users command. This keyword is valid for User authority and does not require an admin session.

Examples The following is an example of the User Accounts command:

```
SANbox2-64 N108 (admin) #> user accounts

  Current list of user accounts
  -----------------------------
  admin        (admin authority = True)
  user1        (admin authority = False)
  user2        (admin authority = False)
  user3        (admin authority = True)
```

The following is an example of the User Add command:

```
SANbox2-64 N108 (admin) #> user add

      Press ’q’ and the ENTER key to abort this command.

  account name (1-15 chars)      : user3
  account password (4-20 chars)  :

  please confirm account password:

  should this account have admin authority? (y/n) [n] : y

  OK to add user account ’user3’ with admin authority?
  Please confirm (y/n): [n] y
```

The following is an example of the User Delete command:

```
SANbox2-64 N108 (admin) #> user del user3

  The user account will be deleted.  Please confirm (y/n): [n] y
```

The following is an example of the User List command:

```
SANbox2-64 N108 (admin) #> user list

  Current list of users logged in
  ------------------------------
  admin@OB-session1 - in admin mode
  admin@OB-session2
  user1@OB-session3

SANbox2-64 N108 (admin) #>
```

Whoami Command

Displays the account name, session number, and switch domain ID for the Telnet session.

Authority User

Syntax **whoami**

Examples The following is an example of the Whoami command:

```
SANbox2-64 N108 #> whoami

User name:admin@session2
Switch name:SANbox2
Switch domain ID:1
```

Zone Command

Manages zones and zone membership on a switch. The Zone command defines members (ports/devices) for a single switch. Zones are members of zone sets.

Authority Admin authority and a Zoning Edit session. Refer to the "Zoning Command" on page B-79 for information about starting a Zoning Edit session. The List, Members, and Zonesets keywords are available with User authority and do not require a Zoning Edit session.

Syntax

zone
add [zone] [members]
copy [zone_source] [zone_destination]
create [zone]
delete [zone]
list
members [zone]
remove [zone] [members]
rename [zone_old [zone_new]
type [zone] *[zone_type]*
zonesets [zone]

Keywords

add [zone] [members]
Specifies one or more ports/devices given by [members] to add to the zone named [zone]. A zone can have a maximum of 256 members. [members] can have one of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs and port numbers are in decimal. Ports are numbered beginning with 0.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

The application verifies that the [members] format is correct, but does not validate that such a port exists.

copy [zone_source] [zone_destination]
Creates a new zone named [zone_destination] and copies the membership into it from the zone given by [zone_source].

create [zone]
Creates a zone with the name given by [zone]. An zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, and -. The zoning database supports a maximum of 1000 zones.

delete [zone]
Deletes the specified zone given by [zone] from the zoning database. If the zone is a member of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all zones and the zone sets of which they are members. This keyword is valid for User authority and does not require a zoning edit session.

members [zone]
Displays all members of the zone given by [zone]. This keyword is available with User authority and does not require a Zoning Edit session.

remove [zone] [members]
Removes the ports/devices given by [members] from the zone given by [zone]. [members] can have one of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs and port numbers are in decimal. Ports are numbered beginning with 0.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

rename [zone_old] [zone_new]
Renames the zone given by [zone_old] to the zone given by [zone_new].

type [zone] *[zone_type]*
Specifies the zone type given by [zone_type] to be assigned to the zone name given by [zone]. If you omit the [zone_type], the system displays the zone type for the zone given by [zone]. [zone_type] can be one of the following:

soft
Name server zone

hardACL
Access control list hard zone. This keyword is case sensitive.

hardVPF
Virtual private fabric hard zone. This keyword is case sensitive.

zonesets [zone]
Displays all zone sets of which the zone given by [zone] is a member. This keyword is available with User authority and does not require a Zoning Edit session.

Examples

The following is an example of the Zone List command:

```
SANbox2-64 N108 #> zone list

  Zone        ZoneSet
  --------------------
  wwn_b0241f
              zone_set_1

  wwn_23bd31
              zone_set_1

  wwn_221416
              zone_set_1

  wwn_2215c3
              zone_set_1

  wwn_0160ed
              zone_set_1

  wwn_c001b0
              zone_set_1

  wwn_401248
              zone_set_1

  wwn_02402f
              zone_set_1

  wwn_22412f
              zone_set_1
```

The following is an example of the Zone Members command:

```
SANbox2-64 N108 #> zone members wwn_b0241f

  Current List of Members for Zone: wwn_b0241f
  --------------------------------
  50:06:04:82:bf:d2:18:c2
  50:06:04:82:bf:d2:18:d2
  21:00:00:e0:8b:02:41:2f
```

The following is an example of the Zone Zonesets command:

```
SANbox2-64 N108 #> zone zonesets zone1

  Current List of ZoneSets for Zone: wwn_b0241f
  --------------------------------
  zone_set_1
```

Zoneset Command

Manages zone sets and zone set membership across the fabric.

Authority Admin authority and a Zoning Edit session. Refer to the "Zoning Command" on page B-79 for information about starting a Zoning Edit session. The Active, List, and Zones keywords are available with User authority. You must close the Zoning Edit session before using the Activate and Deactivate keywords.

Syntax

zoneset
activate [zone_set]
active
add [zone_set] [zone_list]
copy [zone_set_source] [zone_set_destination]
create [zone_set]
deactivate
delete [zone_set]
list
remove [zone_set] [zone_list]
rename [zone_set_old] [zone_set_new]
zones [zone_set]

Keywords

activate [zone_set]
Activates the zone set given by [zone_set]. This keyword deactivates the active zone set. Close the Zoning Edit session before using this keyword.

active
Displays the name of the active zone set. This keyword is available with User authority and does not require a Zoning Edit session.

add [zone_set] [zone_list]
Adds a list of zones and aliases given by [zone_list] to the zone set given by [zone_set]. Zone and alias names are delimited by spaces in [zone_list]. This keyword requires a Zoning Edit session.

copy [zone_set_source] [zone_set_destination]
Creates a new zone set named [zone_set_destination] and copies into it the membership from the zone set given by [zone_set_source]. This keyword requires a Zoning Edit session.

create [zone_set]
Creates the zone set with the name given by [zone_set]. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, and -. This keyword requires a Zoning Edit session. The zoning database supports a maximum of 256 zone sets.

deactivate
Deactivates the active zone set. Close the Zoning Edit session before using this keyword.

delete [zone_set]
Deletes the zone set given by [zone_set]. If the specified zone set is active, the command is suspended until the zone set is deactivated. This keyword requires a Zoning Edit session.

list
Displays a list of all zone sets. This keyword is available with User authority and does not require a Zoning Edit session.

remove [zone_set] [zone_list]
Removes a list of zones given by [zone_list] from the zone set given by [zone_set]. Zone names are delimited by spaces in [zone_list]. If [zone_set] is the active zone set, the zone will not be removed until the zone set has been deactivated. This keyword requires a Zoning Edit session.

rename [zone_set_old] [zone_set_new]
Renames the zone set given by [zone_set_old] to the name given by [zone_set_new]. You can rename the active zone set. This keyword requires a Zoning Edit session.

zones [zone_set]
Displays all zones that are members of the zone set given by [zone_set]. This keyword is available with User authority and does not need a Zoning Edit session.

Notes

- A zone set must be active for its definitions to be applied to the fabric.
- Only one zone set can be active at one time.
- A zone can be a member of more than one zone set.

Examples

The following is an example of the Zoneset Active command:

```
SANbox2-64 N108 #> zoneset active

  The active ZoneSet is:  Beta
```

The following is an example of the Zoneset List command:

```
SANbox2-64 N108 #> zoneset list
  Current List of ZoneSets
  ------------------------
  alpha
  beta
```

The following is an example of the Zoneset Zones command:

```
SANbox2-64 N108 #> zoneset zones ssss
  Current List of Zones for ZoneSet: ssss
  ---------------------------------
  zone1
  zone2
  zone3
```

Zoning Command

Opens a Zoning Edit session in which to create and manage zone sets and zones. Refer to the "Zone Command" on page B-73 and the "Zoneset Command" on page B-77.

Authority Admin. The List keyword is available with User authority.

Syntax

zoning
- active
- cancel
- clear
- edit
- history
- limits
- list
- restore
- save

Keywords

active
Displays membership information for the active zone set including member zones and zone members.

cancel
Closes the current Zoning Edit session. Any unsaved changes are lost.

clear
Clears all inactive zone sets from the volatile edit copy of the zoning database. This keyword does not affect the non-volatile zoning database. However, if you enter the Zoning Clear command followed by the Zoning Save command, the non-volatile zoning database will be cleared from the switch. The preferred method for clearing the zoning database from the switch is the Reset Zoning command.

edit
Opens a Zoning Edit session.

history
Displays a history of zoning modifications including the following:

- Time of the most recent zone set activation or deactivation and the user who performed it
- Time of the most recent modifications to the zoning database and the user who made them.
- Checksum for the zoning database

limits
Displays the maximum limits imposed on the zoning database for the number of zone sets, zones, aliases, members per zone, members per alias, and total members.

list
Lists all fabric zoning definitions. This keyword is available with User authority.

restore
Reverts the changes to the zoning database that have been made during the current Zoning Edit session since the last Zoning Save command was entered.

save
Saves changes made during the current Zoning Edit session. The system will inform you that the zone set must be activated to implement any changes. This does not apply if you entered the Zoning Clear command during the Zoning Edit session.

Examples

The following is an example of the Zoning Edit command:

```
SANbox2-64 N108 #> admin start

SANbox2-64 N108 (admin) #> zoning edit

SANbox2-64 N108  (admin-zoning) #>
.
.
SANbox2-64 N108  (admin-zoning) #> zoning cancel

  Zoning edit mode will be canceled.  Please confirm (y/n): [n]   y

SANbox2-64 N108 (admin) #> admin end
```

The following is an example of the Zoning List command:

```
SANbox2-64 N108 #> zoning list
Active ZoneSet Information

  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f

              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31

              wwn_221416
```

```
                    50:06:04:82:bf:d2:18:c2
                    50:06:04:82:bf:d2:18:d2
                    10:00:00:00:c9:22:14:16

          wwn_2215c3
                    50:06:04:82:bf:d2:18:c2
                    50:06:04:82:bf:d2:18:d2
                    10:00:00:00:c9:22:15:c3

Configured Zoning Information

ZoneSet     Zone      ZoneMember
--------------------------------
wwn
          wwn_b0241f
                    50:06:04:82:bf:d2:18:c2
                    50:06:04:82:bf:d2:18:d2
                    21:00:00:e0:8b:02:41:2f

          wwn_23bd31
                    50:06:04:82:bf:d2:18:c2
                    50:06:04:82:bf:d2:18:d2
                    10:00:00:00:c9:23:bd:31

          wwn_221416
                    50:06:04:82:bf:d2:18:c2
                    50:06:04:82:bf:d2:18:d2
                    10:00:00:00:c9:22:14:16

          wwn_2215c3
                    50:06:04:82:bf:d2:18:c2
                    50:06:04:82:bf:d2:18:d2
                    10:00:00:00:c9:22:15:c3
```

Notes

Glossary

Activity LED

A port LED that indicates when frames are entering or leaving the port.

Alias

A collection of objects that can be zoned together. An alias is not a zone, and can not have a zone or another alias as a member.

AL_PA

Arbitrated Loop Physical Address

Arbitrated Loop

A Fibre Channel topology where ports use arbitration to establish a point-to-point circuit.

Arbitrated Loop Physical Address (AL_PA)

A unique one-byte valid value assigned during loop initialization to each NL_Port on a Loop.

ASIC

Application Specific Integrated Circuit

BootP

A type of network server.

Buffer Credit

A measure of port buffer capacity equal to one frame.

Class 2 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports wit h acknowledgment provided.

Class 3 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment.

Domain ID

User defined name that identifies the switch in the fabric.

E_Port

Expansion port. A switch port that connects to another FC-SW-2 compliant switch.

Expansion Port

See E_Port.

Fabric Management Switch

The switch through which the fabric is managed.

Fabric Name

User defined name associated with the file that contains user list data for the fabric.

Fan Fail LED

An LED that indicates that a cooling fan in the switch is operating below standard.

FC-PLDA

Fibre Channel Private Loop Direct Attach

Flash Memory

Memory on the switch that contains the chassis control firmware.

Frame

Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter.

FRU

Field Replaceable Unit

Heartbeat LED

A chassis LED that indicates the status of the internal switch processor and the results of the Power-On Self-Test.

Initiator

The device that initiates a data exchange with a target device.

In-Order-Delivery

A feature that requires that frames be received in the same order in which they were sent.

Input Power LED

A chassis LED that indicates that the switch logic circuitry is receiving proper DC voltages.

IP

Internet Protocol

LIP

Loop Initialization Primitive sequence

Management Information Base

A set of guidelines and definitions for the Fibre Channel functions.

Management Workstation

PC workstation that manages the fabric through the fabric management switch.

MIB

Management Information Base

NL_Port

Node Loop Port. A Fibre Channel device port that supports arbitrated loop protocol.

N_Port

Node Port. A Fibre Channel device port in a point-to-point or fabric connection.

Output Power LED

A power supply LED that indicates that the power supply is providing DC voltage to the switch.

Over Temperature LED

A chassis LED or a power supply LED that indicates that the switch or power supply is overheating.

Port Status LED

A port LED that indicates device login (or loop initialization) status and data traffic.

POST

Power On Self Test

Power On Self Test (POST)

Diagnostics that the switch chassis performs at start up.

Private Device

A device that can communicate only with other devices on the same loop.

Private Loop

A loop of private devices connected to a single switch port.

SANbox Manager

Switch management application.

SFF

Small Form-Factor transceiver.

SFP

Small Form-Factor Pluggable. A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port.

Small Form Factor

A transceiver device, smaller than a GigaBit Interface Converter, that is permanently attached to the circuit board.

Small Form-Factor Pluggable

A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port.

SNMP

Simple Network Management Protocol

Target

A storage device that responds to an initiator device.

VCCI

Voluntary Control Council for Interference

Worldwide Name (WWN)

A unique 64-bit address assigned to a device by the device manufacturer.

WWN

Worldwide Name

Zone

A set of ports or devices grouped together to control the exchange of information.

Zone Set

A set of zones grouped together. The active zone set defines the zoning for a fabric.

Notes

Index

A

access 3-8
Access Control List zone 3-9
account name 3-11, B-1, B-72
ACL - See Access Control List
Activity LED 2-11
Admin authority 3-11, B-3
Admin command B-4
administrative state
  blade B-25
  port B-39
  switch B-26
air flow 2-14, A-4
alarm
  configuration B-20, B-30
  configuration display B-55
  log B-25, B-44
alias
  add members B-5
  copy B-5
  create B-5
  delete B-5
  delete members B-6
  rename B-6
Alias command B-5
altitude A-4
Arbitrated Loop Physical Address B-38
authority 3-11

B

bandwidth 3-7
beacon B-25
blade
  administrative state B-25
  configuration B-27
  configuration display B-55
  display B-44
  reset B-20
  test B-66
brackets 4-2
broadcast B-44
buffer credits A-2

C

cable 3-1
chassis
  air flow A-4
  diagnostics 5-9
  hardware 2-2
  LEDs 2-6
  marking A-4
  shock A-4
  status B-44
  vibration A-4
classes of service A-1
Command Line Interface 2-15, B-1
command syntax B-2
Config command B-7
configuration
  activate B-7
  backup B-7
  copy B-7
  delete B-7
  edit B-7
  file system error 2-5, 5-2
  list B-7
  remove 5-14
  reset B-20
  restore B-8
  restore default 5-14
  save B-8
controls 2-4
CPU module
  chassis LEDs 2-6
  Ethernet port 2-11
  installation 6-5
  removal 6-3
  serial port 2-12
credits 3-6, A-2
cross-connect blade

description 6-11
installation 6-14
removal 6-12

D

date B-9
Date command B-9
device
cabling 4-15
description 3-1
diagnostics 5-1, A-2
dimensions A-3
distance 3-6
domain ID 3-4, 5-6
domain ID lock 3-4
domains B-45
donor port 3-6, B-45

E

E_Port 2-10, 5-6
emissions standards A-4
environmental
conditions 4-2
specifications A-4
Ethernet
LEDs 2-11
port 2-11
event logging
by component B-35
by port B-36
display B-58
restore defaults B-36
save settings B-36
severity level B-36
start B-37
stop B-37
expansion port 2-10

F

F_Port 2-9
fabric
aggregate bandwidth A-2
latency A-2
management 3-10, A-3
management workstation 4-1
multiple chassis 3-4
point-to-point bandwidth A-2
security 3-11, 4-9
factory defaults 5-14, B-20
Fallback command B-10
fan
description 2-14
installation 6-19
removal 6-18
Fan Fail LED 2-7, 5-10
fatal error 5-1, 5-2
fiber optic cable 3-1
Fibre Channel
ports 2-7
protocols A-1
field replaceable unit 6-1
File Transfer Protocol 2-15, 4-18, 5-3
firmware 4-16
failure 5-2
fallback version B-10
install with CLI 4-17
install with FTP and CLI 4-18
install with SANbox Manager 4-16
load image B-15
unpack image 5-13, B-15
version B-49
FL_Port 2-9
flash memory 2-5, 4-19
frame size A-2
FRU - See Field Replaceable Unit
FTP - See File Transfer Protocol

G

G_Port 2-9
GBIC - See GigaBit Interface Converter
generic ports 2-9
Gigabit Interface Converter 3-1
GL_Port 2-9

H

hard zone 3-8

harmonics A-4
HBA - See Host Bus Adapter
Heartbeat LED 2-6, 5-1
Help command B-11
History command B-12
host bus adapter 3-1
Hotswap command B-13
humidity 4-2, A-4
HyperTerminal application 4-8

I

I/O blade 2-7
  configuration B-27
  installation 6-9
  removal 6-7
  reset B-20
Image command B-15
immunity A-4
initiator device 2-10
Input Power LED 2-6, 5-10
installation 4-2

L

laser specifications A-6
latency 3-2, 3-7, A-2
LED
  Fan Fail 2-7, 5-10
  Heartbeat 2-6, 5-1
  Input Power 2-6, 5-10
  Link Status 2-11
  Output Power 2-13, 5-11
  Over Temperature 2-7, 5-10
  Port Status 2-8, 5-5
  Power Supply Fault 2-13, 5-11
link state database B-45
Link Status LED 2-11
Lip command B-16
log
  copy 5-14
  event B-35, B-58
  power-on self test B-48
login limit B-1
Loop Port Bypass B-38
Loop Port Enable B-38

M

maintainability A-2
maintenance
  interface A-3
  menu 5-13
  mode 5-2, 5-3, 5-12
  strategy A-2
Maintenance button 2-5, 5-12
manufacturer information B-62
marking A-4
media type A-2
memory
  activity B-45
  flash 2-5
minicom 4-9

N

name server
  display B-45
  zone 3-9
network
  configuration reset B-20
  interfaces B-45
non-fatal error 5-1

O

Output Power LED 2-13, 5-11
Over Temperature LED 2-7, 5-10

P

page break B-26
Passwd command B-17
password
  change B-17
  file reset 5-14
  restore default 5-14
  user account 3-11, B-1
performance 3-6
planning 3-1
port
  activity 2-8

administrative state B-39
buffer credits 3-6
configuration 4-15, B-27
configuration display B-55
counters B-38
diagnostics 5-5
Ethernet 2-11
Fibre Channel 2-7
generic 2-9
initialize B-20
logged-in status 2-8
loopback test B-66
maximum number of ports/users A-1
modes 2-9
number 2-3
operational information B-46
performance B-46, B-60
serial 2-12
speed A-2, B-38
Port Status LED 2-8, 5-5
POST - See Power On Self Test
power
cords 4-2
down switch 4-19
requirements 4-1
source loading A-3
power on self test
description 5-1
log B-48
Power Supply Fault LED 2-13
power supply module
description 2-13
installation 6-17
removal 6-16
principal
priority 3-4
switch 3-4
Ps command B-18

Q

Quit command B-19

R

rack mount 4-3
recovering a switch 5-12
redundancy 3-2
regulatory certifications A-4
remake filesystem 5-14
removal/replacement 6-1
Reset command B-20
RS-232 port 2-12

S

safety standards A-4
SANbox Manager 2-15
SANbox Manager installation
Linux 4-11, 4-13
Solaris 4-12, 4-13
Windows 4-10, 4-13
scalability A-1
security 3-11, 4-9
serial port 2-12
Set command B-25
Set Config command B-27
Set Log command B-35
Set Port command B-38
Set Setup command B-40
SFP - See Small Form-Factor Pluggable
Show command B-44
Show Config command B-55
Show Log command B-58
Show Perf command B-60
Show Setup command B-62
Shutdown command B-65
Simple Network Management Protocol
configuration B-40
configuration display B-62
description 2-15
reset B-20
site requirements 4-1
slot number 2-3, B-49
small form-factor pluggable 2-8, 6-1
SNMP - See Simple Network Management Protocol
soft zone 3-9

steering B-49
switch
  administrative state B-26
  configuration 4-14, B-29, B-55
  configuration display B-55
  initialize B-20
  management 2-15
  power down 4-19
  recovery 5-12
  reset 5-14, B-69
  specifications A-1
system
  error 5-2
  process B-18
  processor A-2
system configuration
  change B-41
  display B-62

T

target device 2-10
temperature 4-2, A-4, B-44
Test command B-66
time B-9
timeout value 5-6
TL_Port
  devices 2-10
  name server registration 2-10
  number of off-loop devices 2-10
  private initiators 2-10
  private targets 2-10
transceiver 2-8, 4-5, 6-1
translation entries list 2-10
transmission rate 3-6, 3-7

U

Uptime command B-69
user
  account 3-11, B-70
  authority 3-11, B-3
  interface A-2
  logged in B-49
User command B-70

V

ventilation 2-14
vibration A-4
Virtual Private Fabric zone 3-10
voltage
  fluctuations A-4
  operating A-3
VPF - See Virtual Private Fabric

W

Whoami command B-72
workstation 4-1
worldwide name 2-10, 3-8
WWN - See World Wide Name

Z

zone
  Access Control List 3-9
  add member port B-73
  conflict 5-7
  copy B-73
  create B-73
  definition 3-8
  delete B-73
  delete member port B-74
  name server 3-9
  rename B-74
  type B-74
  Virtual Private Fabric 3-10
Zone command B-73
zone set
  activate B-77
  add member zone B-77
  copy B-77
  create B-77
  deactivate B-21, B-77
  delete B-78
  delete member zone B-78
  display B-78
  display active B-77
  display members B-78
  display zones B-74
  rename B-78

Zoneset command B-77
zoning
  configuration B-31
  configuration display B-55
  database B-21
  edit B-79
  history B-79
  limits 3-8, B-79
  list definitions B-80
  save edits B-80
Zoning command B-79